





Join a community dedicated to learning open source

The Red Hat® Learning Community is a collaborative platform for users to accelerate open source skill adoption while working with Red Hat products and experts.



Network with tens of thousands of community members



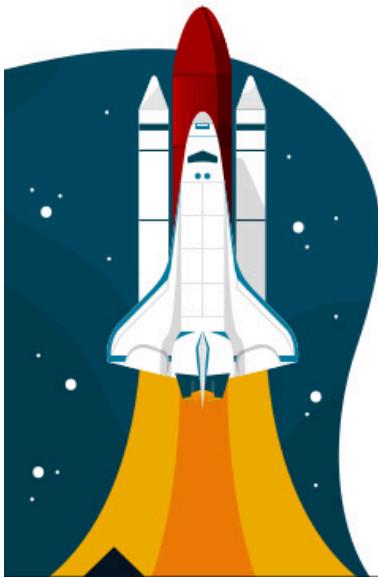
Engage in thousands of active conversations and posts



Join and interact with hundreds of certified training instructors



Unlock badges as you participate and accomplish new goals



This knowledge-sharing platform creates a space where learners can connect, ask questions, and collaborate with other open source practitioners.

Access free Red Hat training videos

Discover the latest Red Hat Training and Certification news

Connect with your instructor - and your classmates - before, after, and during your training course.

Join peers as you explore Red Hat products

Join the conversation learn.redhat.com



Copyright © 2020 Red Hat, Inc. Red Hat, Red Hat Enterprise Linux, the Red Hat logo, and Ansible are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

Seguimiento rápido de RHCSA



Red Hat Enterprise Linux 9.0 RH199

Seguimiento rápido de RHCSA

Edición 4 20221003

fecha de publicación 20221003

Autores: Ashish Lingayat, Bernardo Gargallo, Ed Parenti, Jacob Pelchat,

Mike Kelly, Morgan Weetman, Patrick Gomez

Editor: Julian Cable

Copyright © 2022 Red Hat, Inc.

The contents of this course and all its modules and related materials, including handouts to audience members, are
Copyright © 2022 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 send email to training@redhat.com or phone toll-free (USA) +1 (866) 626-2994 or +1 (919) 754-3700.

Red Hat, Red Hat Enterprise Linux, the Red Hat logo, JBoss, OpenShift, Fedora, Hibernate, Ansible, CloudForms, RHCA, RHCE, RHCSA, Ceph, and Gluster are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries 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 American, Inc. and/or its affiliates.

XFS® is a registered trademark of Hewlett Packard Enterprise Development LP or its subsidiaries in the United States and/or other countries.

MySQL® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js® is a trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack word mark and the Square O Design, together or apart, are trademarks or registered trademarks of OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. Red Hat, Inc. is not affiliated with, endorsed by, or sponsored by the OpenStack Foundation or the OpenStack community.

All other trademarks are the property of their respective owners.

Colaboradores: Adarsh Krishnan, David Sacco, Hemant Chauhan, Roberto Velazquez, Sajith Eyamkuzhy, Samik Sanyal, Yuvaraj Balaraju

Convenciones del documento	xi
	xi
Introducción	xiii
Seguimiento rápido de RHCSA	xiii
Orientación sobre el entorno del aula	xv
Realización de ejercicios de laboratorio	xx
1. Sistemas de acceso y obtención de soporte	1
Edición de archivos de texto desde el prompt de shell	2
Ejercicio Guiado: Edición de archivos de texto desde el prompt de shell	6
Configurar autenticación basada en claves de SSH	8
Ejercicio Guiado: Configurar autenticación basada en claves de SSH	15
Obtención de ayuda en el portal de clientes de Red Hat	21
Ejercicio Guiado: Obtención de ayuda en el portal de clientes de Red Hat	27
Detección y resolución de problemas con Red Hat Insights	29
Cuestionario: Detección y resolución de problemas con Red Hat Insights	36
Resumen	38
2. Administrar archivos desde la línea de comandos	39
Descripción de conceptos de la jerarquía del sistema de archivos Linux	40
Cuestionario: Descripción de conceptos de la jerarquía del sistema de archivos Linux	43
Creación de enlaces entre archivos	47
Ejercicio Guiado: Creación de enlaces entre archivos	51
Coincidencia de nombres de archivo con expansiones de shell	53
Cuestionario: Coincidencia de nombres de archivo con expansiones de shell	58
Trabajo de laboratorio: Administrar archivos desde la línea de comandos	62
Resumen	72
3. Administración de usuarios y grupos locales	73
Describir conceptos de usuario y grupo	74
Cuestionario: Describir conceptos de usuario y grupo	78
Obtención de acceso de superusuario	82
Ejercicio Guiado: Obtención de acceso de superusuario	88
Administración de cuentas de usuarios locales	93
Ejercicio Guiado: Administración de cuentas de usuarios locales	96
Administración de cuentas de grupos locales	99
Ejercicio Guiado: Administración de cuentas de grupos locales	102
Administración de contraseñas de usuarios	105
Ejercicio Guiado: Administración de contraseñas de usuarios	109
Trabajo de laboratorio: Administración de usuarios y grupos locales	114
Resumen	120
4. Control de acceso a los archivos	121
Administración de permisos del sistema de archivos desde la línea de comandos	122
Ejercicio Guiado: Administración de permisos del sistema de archivos desde la línea de comandos	127
Administración de permisos predeterminados y acceso a archivos	130
Ejercicio Guiado: Administración de permisos predeterminados y acceso a archivos	135
Trabajo de laboratorio: Control de acceso a los archivos	139
Resumen	146
5. Administración de seguridad de SELinux	147
Cambio del modo de cumplimiento (enforcement) de SELinux	149
Ejercicio Guiado: Cambio del modo de cumplimiento (enforcement) de SELinux	154
Control de contextos de archivo de SELinux	157
Ejercicio Guiado: Control de contextos de archivo de SELinux	162
Ajuste de la política de SELinux con booleanos	165

Ejercicio Guiado: Ajuste de la política de SELinux con booleanos	168
Investigación y resolución de problemas de SELinux	171
Ejercicio Guiado: Investigación y resolución de problemas de SELinux	176
Trabajo de laboratorio: Administración de seguridad de SELinux	180
Resumen	186
6. Ajuste del rendimiento del sistema	187
Finalización de procesos	188
Ejercicio Guiado: Finalización de procesos	194
Monitoreo de la actividad de procesos	198
Ejercicio Guiado: Monitoreo de la actividad de procesos	202
Ajuste de perfiles de optimización	207
Ejercicio Guiado: Ajuste de perfiles de optimización	214
Influencia en la programación de procesos	219
Ejercicio Guiado: Influencia en la programación de procesos	224
Trabajo de laboratorio: Ajuste del rendimiento del sistema	228
Resumen	234
7. Programación de tareas futuras	235
Programación de trabajos de usuario recurrentes	236
Ejercicio Guiado: Programación de trabajos de usuario recurrentes	239
Programación de trabajos del sistema recurrentes	242
Ejercicio Guiado: Programación de trabajos del sistema recurrentes	246
Administración de archivos temporales	249
Ejercicio Guiado: Administración de archivos temporales	253
Cuestionario: Programación de tareas futuras	256
Resumen	260
8. Instalación y actualización de paquetes de software	261
Registro de sistemas para Soporte de Red Hat	262
Cuestionario: Registro de sistemas para Soporte de Red Hat	266
Instalación y actualización de paquetes de software con DNF	268
Ejercicio Guiado: Instalación y actualización de paquetes de software con DNF	277
Habilitar repositorios de software con DNF	282
Ejercicio Guiado: Habilitar repositorios de software con DNF	285
Trabajo de laboratorio: Instalación y actualización de paquetes de software	289
Resumen	295
9. Administración de almacenamiento básico	297
Montaje y desmontaje de sistemas de archivos	298
Ejercicio Guiado: Montaje y desmontaje de sistemas de archivos	302
Adición de particiones, sistemas de archivos y montajes persistentes	305
Ejercicio Guiado: Adición de particiones, sistemas de archivos y montajes persistentes	315
Administración de espacio de intercambio (swap)	319
Ejercicio Guiado: Administración de espacio de intercambio (swap)	324
Trabajo de laboratorio: Administración de almacenamiento básico	328
Resumen	336
10. Administración de la pila (stack) de almacenamiento	337
Creación y ampliación de volúmenes lógicos	338
Ejercicio Guiado: Creación y ampliación de volúmenes lógicos	349
Administración de almacenamiento en capas	355
Ejercicio Guiado: Administración de almacenamiento en capas	362
Trabajo de laboratorio: Administración de la pila (stack) de almacenamiento	368
Resumen	374
11. Servicios de control y proceso de arranque	375
Identificación de procesos del sistema iniciados en forma automática	376

Ejercicio Guiado: Identificación de procesos del sistema iniciados en forma automática ...	382
Control de servicios del sistema	386
Ejercicio Guiado: Control de servicios del sistema	391
Selección del objetivo de arranque	395
Ejercicio Guiado: Selección del objetivo de arranque	401
Restablecimiento de la contraseña de root	404
Ejercicio Guiado: Restablecimiento de la contraseña de root	409
Reparación de problemas del sistema de archivos en el arranque	411
Ejercicio Guiado: Reparación de problemas del sistema de archivos en el arranque	414
Trabajo de laboratorio: Control del proceso de arranque	417
Resumen	423
12. Analizar y almacenar registros	425
Descripción de la arquitectura de registro del sistema	426
Cuestionario: Descripción de la arquitectura de registro del sistema	428
Revisión de archivos Syslog	432
Ejercicio Guiado: Revisión de archivos Syslog	437
Revisión de las entradas del diario (journal) del sistema	439
Ejercicio Guiado: Revisión de las entradas del diario (journal) del sistema	445
Resguardo del diario (journal) del sistema	448
Ejercicio Guiado: Resguardo del diario (journal) del sistema	451
Mantenimiento de la hora correcta	454
Ejercicio Guiado: Mantenimiento de la hora correcta	458
Trabajo de laboratorio: Analizar y almacenar registros	462
Resumen	468
13. Administración de redes	469
Validación de la configuración de red	470
Ejercicio Guiado: Validación de la configuración de red	476
Configuración de redes desde la línea de comandos	479
Ejercicio Guiado: Configuración de redes desde la línea de comandos	486
Edición de archivos de configuración de red	492
Ejercicio Guiado: Edición de archivos de configuración de red	496
Configuración de nombres de host y resolución de nombre	500
Ejercicio Guiado: Configuración de nombres de host y resolución de nombre	504
Trabajo de laboratorio: Administración de redes	508
Resumen	513
14. Acceso al almacenamiento conectado a la red	515
Administración de almacenamiento conectado a la red con NFS	516
Ejercicio Guiado: Administración de almacenamiento conectado a la red con NFS	520
Montaje automático de almacenamiento conectado a la red	524
Ejercicio Guiado: Montaje automático de almacenamiento conectado a la red	529
Trabajo de laboratorio: Acceso al almacenamiento conectado a la red	535
Resumen	542
15. Administración de la seguridad de redes	543
Administración de firewalls del servidor	544
Ejercicio Guiado: Administración de firewalls del servidor	552
Trabajo de laboratorio: Administración de la seguridad de redes	555
Resumen	563
16. Ejecución de contenedores	565
Conceptos de contenedores	566
Cuestionario: Conceptos de contenedores	573
Implementación de contenedores	577
Ejercicio Guiado: Implementación de contenedores	587

Administración del almacenamiento del contenedor y los recursos de red	593
Ejercicio Guiado: Administración del almacenamiento del contenedor y los recursos de red	604
Administración de contenedores como servicios del sistema	610
Ejercicio Guiado: Administración de contenedores como servicios del sistema	617
Trabajo de laboratorio: Ejecución de contenedores	623
Resumen	630
17. Revisión exhaustiva	631
Revisión exhaustiva	632
Trabajo de laboratorio: Corrección de problemas de arranque y mantenimiento de servidores	637
Trabajo de laboratorio: Configuración y administración de sistemas de archivos y almacenamiento	644
Trabajo de laboratorio: Configuración y administración de seguridad del servidor	650
Trabajo de laboratorio: Ejecución de contenedores	660

Convenciones del documento

En esta sección, se describen diversas convenciones y prácticas usadas en todos los cursos de capacitación de Red Hat.

Admoniciones

En los cursos de capacitación de Red Hat, se usan las siguientes admoniciones:



Referencias

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



nota

Las "Notas" son consejos, atajos o enfoques alternativos para una tarea determinada. Ignorar una nota no debería tener consecuencias negativas, pero podría pasarse por alto algún truco que puede simplificar una tarea.



Importante

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. Ignorar estas admoniciones no provocará pérdida de datos, pero podría causar irritación y frustración.



Advertencia

No se deben ignorar las advertencias. Es muy probable que ignorar estas admoniciones provoque pérdida de datos.

Lenguaje inclusivo

La capacitación de Red Hat actualmente está revisando su uso del lenguaje en diversas áreas para ayudar a eliminar cualquier término que pueda ser ofensivo. Se trata de un proceso continuo y requiere la alineación con los productos y servicios que se abordan en los cursos de capacitación de Red Hat. Red Hat agradece su paciencia durante este proceso.

Introducción

Seguimiento rápido de RHCSA

El curso *Red Hat Certified System Administrator Rapid Track (RH199)* está diseñado como un curso de capacitación rápida sobre administración de sistemas de Red Hat Enterprise Linux para profesionales de TI con una exposición significativa a Linux. Los estudiantes con un conocimiento básico de la línea de comandos de Linux aprenderán las tareas clave para administrar un solo sistema Red Hat Enterprise Linux. Este curso es un curso acelerado. Cuando se imparte como un curso dirigido por un instructor, este curso cubre el contenido de capacitación en 5 días que normalmente se cubre durante 10 días en *Red Hat System Administration I* y *Red Hat System Administration II*. Algunos conceptos de esos otros dos cursos se tratan solo brevemente en este curso o no se tratan.

Objetivos del curso

- Ampliar las habilidades obtenidas durante el curso *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)* está diseñado como un curso de capacitación rápida sobre administración de sistemas de Red Hat Enterprise Linux para profesionales de TI con una exposición significativa a Linux. Los estudiantes deben sentirse cómodos con la ejecución de comandos comunes de Linux desde el prompt de shell. Se recomienda encarecidamente a los estudiantes que no tengan este conocimiento que realicen *Red Hat System Administration I (RH124)*.

Requisitos previos

Se espera que se sienta cómodo con la siguiente lista de actividades:

- Crear archivos y directorios con rutas relativas y absolutas.
- Copiar y mover archivos.
- Crear y restaurar archivos de almacenamiento.
- Interpretar los permisos del sistema de archivos.
- Localizar archivos en el sistema.
- Redactar scripts de Bash simples.

Orientación sobre el entorno del aula

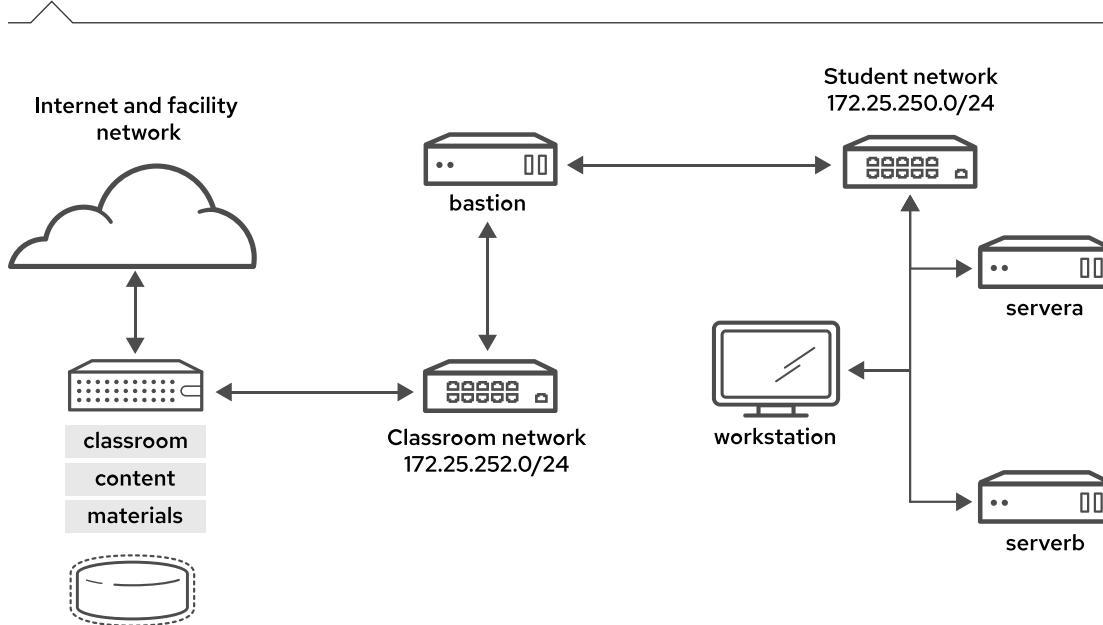


Figura 0.1: Entorno del aula

En este curso, el sistema de cómputo principal usado para las actividades prácticas de aprendizaje es **workstation**. Los estudiantes también usan otras dos máquinas para estas actividades: **servera** y **serverb**. Estos tres sistemas se encuentran en el dominio DNS `lab.example.com`.

Todos los sistemas de cómputo de los estudiantes tienen una cuenta de usuario estándar (`student`) con la contraseña `student`. La contraseña `root` de todos los sistemas de los estudiantes es `redhat`.

Máquinas del aula

Nombre de la máquina	Direcciones IP	Rol
<code>bastion.lab.example.com</code>	172.25.250.254	Sistema de puerta de enlace para conectar la red privada de los estudiantes al servidor del aula (debe estar siempre en ejecución)
<code>workstation.lab.example.com</code>	172.25.250.9	Estación de trabajo gráfica para la administración del sistema
<code>servera.lab.example.com</code>	172.25.250.10	Servidor administrado "A"
<code>serverb.lab.example.com</code>	172.25.250.11	Servidor administrado "B"

La función principal de `bastion` es actuar como enrutador entre la red que conecta las máquinas de los estudiantes y la red del aula. Si `bastion` está apagada, las máquinas de los estudiantes solo podrán acceder a sistemas en la red de estudiantes individuales.

Varios sistemas en el aula brindan servicios de soporte. Dos servidores, `content.example.com` y `materials.example.com`, son fuentes de software y materiales del trabajo de laboratorio usados en actividades prácticas. Se provee información sobre cómo usar estos servidores en las instrucciones para estas actividades. Estas actividades las proporciona la máquina virtual `workstation`. Tanto `classroom` como `bastion` se deben estar ejecutando siempre para el uso adecuado del entorno de laboratorio.



nota

Al iniciar sesión en `serverao` o `serverb` es posible que vea un mensaje sobre la activación de `cockpit`. Puede ignorar los mensajes.

```
[student@workstation ~]$ ssh student@serverb
Warning: Permanently added 'serverb,172.25.250.11' (ECDSA) to the list of
known hosts.
Activate the web console with: systemctl enable --now cockpit.socket

[student@serverb ~]$
```

Control de las máquinas virtuales

Se le asignan computadoras remotas en un aula de aprendizaje en línea de Red Hat (Red Hat Online Learning Environment, ROLE). Se accede a los cursos de autoaprendizaje a través de una aplicación web alojada en `rol.redhat.com` [<http://rol.redhat.com>]. Inicie sesión en este sitio con sus credenciales de usuario del Portal de clientes de Red Hat.

Control de las máquinas virtuales

Las máquinas virtuales del entorno de su aula se controlan a través de controles de interfaz en la página web. El estado de cada máquina virtual en el aula se muestra en la pestaña **Lab Environment**.

The screenshot shows a user interface for managing a lab environment. At the top, there are tabs for 'Table of Contents', 'Course', 'Lab Environment', and icons for a star and help. Below this is a section titled 'Lab Controls' with instructions: 'Click CREATE to build all of the virtual machines needed for the classroom lab environment. This may take several minutes to complete. Once created the environment can then be stopped and restarted to pause your experience.' It also states that deleting the lab will remove all virtual machines and lose progress. A large button labeled 'STOP' is prominent. Below these controls is a table listing five virtual machines:

VM Name	Status	Action	Open Console
bastion	active	ACTION -	OPEN CONSOLE
classroom	active	ACTION -	OPEN CONSOLE
servera	building	ACTION -	OPEN CONSOLE
serverb	building	ACTION -	OPEN CONSOLE
workstation	active	ACTION -	OPEN CONSOLE

Figura 0.2: Ejemplo de la página de gestión del Entorno de laboratorio de un curso

Estados de la máquina

Estado de la máquina virtual	Descripción
building (en construcción)	La máquina virtual se está creando.
active (activa)	La máquina virtual se está ejecutando y está disponible. Si acaba de arrancar, podría estar iniciando servicios todavía.
stopped (detenida)	La máquina virtual se ha apagado completamente. Al iniciarse, la máquina virtual arranca en el mismo estado en que se hallaba antes de apagarse. El estado del disco se conserva.

Acciones del aula

Botón o acción	Descripción
CREATE	Crea el aula de ROLE. Crea e inicia todas las máquinas virtuales necesarias para esta aula. La creación puede tardar varios minutos en completarse.
CREATING	Se están creando las máquinas virtuales del aula de ROLE. Crea e inicia todas las máquinas virtuales que son necesarias para esta aula. La creación puede tardar varios minutos en completarse.
DELETE	Elimina el aula de ROLE. Destruye todas las máquinas virtuales del aula. Se perderá todo el trabajo guardado en los discos del sistema.
START	Inicia todas las máquinas virtuales en el aula.
STARTING	Todas las máquinas virtuales en el aula se están iniciando.

Botón o acción	Descripción
STOP	Detiene todas las máquinas virtuales en el aula.

Acciones de la máquina

Botón o acción	Descripción
OPEN CONSOLE	Se conecta con la consola del sistema de la máquina virtual en una nueva pestaña del navegador. Puede iniciar sesión directamente en la máquina virtual y ejecutar los comandos cuando sea necesario. Habitualmente, debe iniciar sesión solo en la máquina virtual <code>workstation</code> y usar desde allí <code>ssh</code> para conectarse con las otras máquinas virtuales.
ACTION > Start	Inicie (power on [encender]) la máquina virtual.
ACTION > Shutdown	Apaga la máquina virtual correctamente y preserva el contenido del disco.
ACTION > Power Off	Fuerza el apagado de la máquina virtual al tiempo que preserva el contenido del disco. Esto equivale a desenchufar una máquina física.
ACTION > Reset	Fuerza el apagado de la máquina virtual y restablece el almacenamiento asociado para que vuelva a su estado original. Se perderá todo el trabajo guardado en los discos del sistema.

Al inicio de un ejercicio, si se le indica que restablezca el nodo de una máquina virtual, haga clic en **ACTION > Reset** solo para esa máquina virtual específica.

Al inicio de un ejercicio, si se le indica que restablezca todas las máquinas virtuales, haga clic en **ACTION (ACCIÓN) > Reset (Restablecer)** en cada máquina virtual de la lista.

Si desea que el entorno del aula vuelva a su estado original al inicio del curso, haga clic en **DELETE** para suprimir el entorno del aula completo. Después de eliminar el trabajo de laboratorio, haga clic en **CREATE** para aprovisionar un nuevo conjunto de sistemas del aula.



Advertencia

La operación **DELETE** (ELIMINAR TRABAJO DE LABORATORIO) no puede deshacerse. Se perderá todo el trabajo que haya completado en el entorno del aula.

Temporizadores de detención automática y eliminación automática

La inscripción al aprendizaje en línea de Red Hat le otorga derecho a un cierto tiempo de uso del equipo. Para ayudarlo a conservar el tiempo asignado, el aula de ROLE usa temporizadores, que apagan o eliminan el entorno del aula cuando el temporizador correspondiente caduca.

Para ajustar los temporizadores, ubique los dos botones + en la parte inferior de la página de administración del curso. Haga clic en el botón + de detención automática para agregar otra hora al temporizador de detención automática. Haga clic en el botón + de eliminación automática para agregar otro día al temporizador de eliminación automática. La detención automática tiene un tiempo máximo de 11 horas, y la eliminación automática un tiempo máximo de 14 días. Preste

atención y mantenga los temporizadores configurados mientras trabaja, de forma tal que el entorno no se apague de manera imprevista. Tenga cuidado de no establecer los temporizadores en tiempos innecesariamente prolongados, ya que podría perder el tiempo de suscripción asignado.

Realización de ejercicios de laboratorio

Es posible que vea los siguientes tipos de actividades de laboratorio en este curso:

- Un *ejercicio guiado* es un ejercicio práctico que sigue a una sección de presentación. Lo guía paso a paso para realizar un procedimiento.
- Un *cuestionario* se suele usar para corroborar el aprendizaje de los conocimientos o cuando una actividad práctica resulta poco práctica por algún otro motivo.
- Un *trabajo de laboratorio al final del capítulo* es una actividad práctica que se puede calificar para ayudarlo a verificar su aprendizaje. Usted trabajará en una serie de pasos de alto nivel, los cuales están basados en los ejercicios guiados de ese capítulo, pero los pasos no lo guiarán en cada comando. Se proporciona una solución con un tutorial paso a paso.
- Se usa un *trabajo de laboratorio con revisión integral* al final del curso. También es una actividad práctica que se puede calificar y puede abarcar el contenido de todo el curso. Usted trabaja en una especificación de lo que debe lograr en la actividad, sin recibir los pasos específicos para hacerlo. Reiteramos: se proporciona una solución con un tutorial paso a paso que cumple la especificación.

Para preparar su entorno de laboratorio al inicio de cada actividad práctica, ejecute el comando `lab start` con el nombre de actividad especificado de las instrucciones de la actividad. Del mismo modo, al final de cada actividad práctica, ejecute el comando `lab finish` con el mismo nombre de actividad para eliminar todo después de la actividad. Cada actividad práctica tiene un nombre único dentro de un curso.

La sintaxis para ejecutar un script de ejercicio es la siguiente:

```
[student@workstation ~]$ lab action exercise
```

Las acciones son `start` (iniciar), `grade` (calificar) o `finish` (finalizar). Todos los ejercicios soportan las acciones `start` (iniciar) y `finish` (finalizar). Solo los trabajos de laboratorio al final del capítulo y los trabajos de laboratorio con revisión integral soportan la acción `grade` (calificar).

start (iniciar)

La acción `start` verifica los recursos necesarios para comenzar un ejercicio. Esto podría incluir los ajustes de configuración, la creación de recursos, la verificación de los servicios con requisitos previos y la verificación de los resultados necesarios de los ejercicios anteriores. Puede realizar un ejercicio en cualquier momento, incluso sin realizar los ejercicios anteriores.

grade (calificar)

Para las actividades calificables, la acción `grade` dirige el comando `lab` para evaluar su trabajo y muestra una lista de criterios de calificación con un estado `PASS` o `FAIL` para cada uno. Para que el estado sea `PASS` en todos los criterios, corrija los errores y vuelva a ejecutar la acción `grade`.

finish (finalizar)

La acción `finish` elimina los recursos que se configuraron durante el ejercicio. Puede realizar un ejercicio tantas veces como desee.

El comando `lab` admite la finalización con tabulación. Por ejemplo, para enumerar todos los ejercicios que puede iniciar, ingrese `lab start` y, luego, presione la tecla Tab dos veces.

capítulo 1

Sistemas de acceso y obtención de soporte

Meta

Edite archivos de texto, inicie sesión en el sistema Linux local y remoto, e investigue los métodos de resolución de problemas proporcionados a través de Red Hat Support y Red Hat Insights.

Objetivos

- Crear y editar archivos de texto desde la línea de comandos con el editor vim.
- Configurar una cuenta de usuario para usar autenticación basada en claves para iniciar sesión en sistemas remotos de forma segura y sin una contraseña.
- Describir y usar los recursos clave en el portal de clientes de Red Hat para encontrar información en la documentación y la base de conocimientos de Red Hat.
- Usar Red Hat Insights para analizar los servidores en busca de problemas, corregirlos o resolverlos, y confirmar que la solución haya funcionado.

Secciones

- Edición de archivos de texto desde el prompt de shell (y ejercicio guiado)
- Configuración de autenticación basada en claves de SSH (y ejercicio guiado)
- Obtener ayuda en el portal de clientes de Red Hat (y ejercicio guiado)
- Detectar y resolver problemas con Red Hat Insights (y cuestionario)

Edición de archivos de texto desde el prompt de shell

Objetivos

Crear y editar archivos de texto desde la línea de comandos con el editor `vim`.

Editar archivos con Vim

Un principio fundamental de diseño de Linux es que la configuración y la información se almacenan en archivos basados en texto. Estos archivos siguen diversas estructuras, como listas de configuraciones, formatos tipo INI, XML o YAML estructurados, etc. La ventaja de almacenar archivos en una estructura basada en texto es que se pueden editar fácilmente con cualquier editor de texto simple.

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

Ventajas del editor Vim

Cuando un sistema usa un prompt de shell de solo texto, debe saber cómo usar al menos un editor de texto para editar archivos. Así, puede editar archivos de configuración basados en texto desde una ventana de terminal o desde inicios de sesión remotos a través del comando `ssh` o de la consola web. Tampoco necesitará acceso a un escritorio gráfico para editar archivos en un servidor, y es posible que ese servidor no necesite ejecutar un entorno de escritorio gráfico.

La razón clave para aprender a usar Vim es que casi siempre se instala de manera predeterminada en un servidor para editar archivos basados en texto. La *Interfaz de sistema operativo portátil* o estándar *POSIX* especificaba el editor `vi` en Linux, y muchos otros sistemas operativos similares a UNIX hacen lo mismo.

Además, Vim se usa a menudo como la implementación de `vi` en otros sistemas operativos o distribuciones comunes. Por ejemplo, macOS actualmente incluye una instalación ligera de Vim de forma predeterminada. Por lo tanto, las habilidades de Vim que se aprenden para Linux también pueden resultar útiles en otros lugares.

Introducción a Vim

Puede instalar el editor Vim en Red Hat Enterprise Linux con cualquiera de los dos paquetes. Estos dos paquetes proporcionan diferentes funciones y comandos de Vim para editar archivos basados en texto.

Con el paquete `vim-minimal`, puede instalar el editor `vi` con funciones centrales (core). Esta es una instalación muy ligera que incluye solo el conjunto de características centrales (core) y el comando básico `vi`. Puede abrir un archivo para editarlo con el comando `vi`.

```
[user@host ~]$ vi filename
```

De manera alternativa, puede usar el paquete `vim-enhanced` para instalar el editor de Vim. Este paquete proporciona un conjunto de características mucho más completo, un sistema de ayuda en línea, y un programa tutorial. Para iniciar Vim en este modo mejorado, use el comando `vim`.

```
[user@host ~]$ vim filename
```

Las funciones centrales (core) del editor Vim están disponibles en ambos comandos.

Si `vim-enhanced` está instalado, se configura un alias de shell para que si los usuarios normales ejecutan el comando `vi`, obtienen automáticamente el comando `vim` en su lugar. Esto no se aplica a `root` y otros usuarios con UID por debajo de 200 (que usan los servicios del sistema).

Si `vim-enhanced` está instalado y un usuario regular desea usar el comando `vi`, es posible que tenga que usar el comando `\vi` para anular el alias temporalmente. Puede usar `\vi --version` y `vim --version` para comparar los conjuntos de características de los dos comandos.

Modos de operación de Vim

El editor Vim ofrece diversos modos de operación, como el *modo de comando*, el *modo de comando extendido*, el *modo de edición* y el *modo visual*. Debería estar siempre al tanto del modo actual, ya que las pulsaciones de teclas tienen diferentes efectos en los diferentes modos.

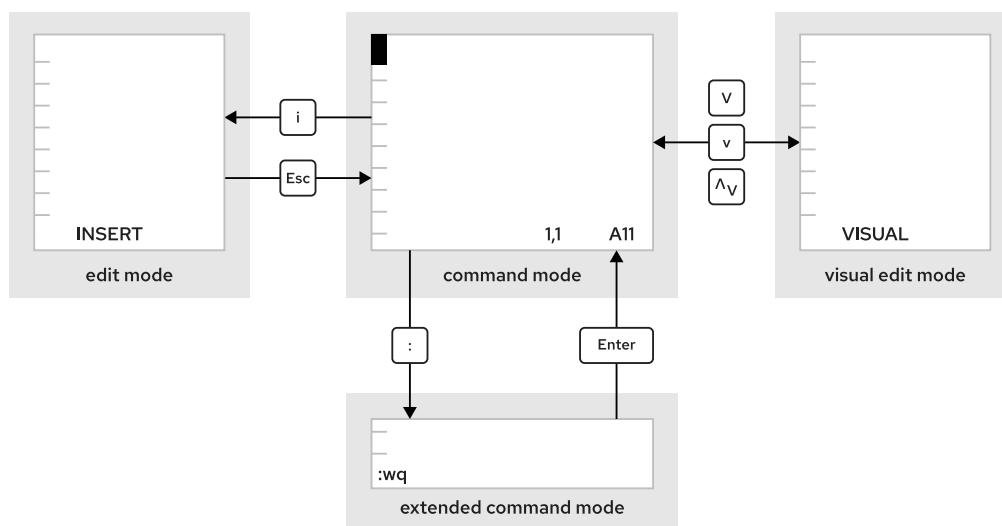


Figura 1.1: Cambio entre modos de Vim

Cuando se abre Vim por primera vez, arranca en el *modo de comando*, usado para navegar, cortar y pegar, y otro tipo de modificación de texto. Al presionar la tecla requerida se accede a funciones de edición específicas.

- Una pulsación de la tecla `i` ingresa al *modo de inserción*, en el cual todo el texto ingresado se convierte en contenido de archivo. Al presionar `Esc` se vuelve al modo comando.
- Al pulsar la tecla `v` se ingresa al *modo visual*, en el cual se pueden seleccionar varios caracteres para la manipulación de texto. Use `Shift+V` para líneas múltiples y `Ctrl+V` para seleccionar en bloque. Para salir del modo visual, use las teclas `v`, `Shift+V` o `Ctrl+V`.
- Al pulsar la tecla `:` se inicia el *modo de comando ampliado* para tareas como la escritura del archivo (para guardarlo) y la salida del editor Vim.

**nota**

Si no está seguro del modo que Vim está usando, presione Esc un par de veces para volver al modo de comandos. Es seguro presionar la tecla Esc en modo comando repetidamente.

Flujo de trabajo mínimo y básico de Vim

Vim tiene pulsaciones de teclas eficaces, coordinadas para tareas de edición avanzadas. Aunque se las considera beneficiosas con la práctica, las capacidades de Vim pueden abrumar a los nuevos usuarios.

Red Hat recomienda aprender las siguientes teclas y comandos de Vim.

- La tecla **u** deshace la edición más reciente.
- La tecla **x** borra un solo carácter.
- El comando **:w** escribe (guarda) el archivo y permanece en el modo de comandos para seguir editando.
- El comando **:wq** escribe (guarda) el archivo y sale de Vim.
- El comando **:q!** sale de Vim y descarta todos los cambios que se realizaron al archivo desde la última escritura.

Aprender estos comandos ayuda a un usuario de Vim a realizar cualquier tarea de edición.

Reorganización de texto existente

En Vim, puede *tirar* y *colocar* (copiar y pegar) usando los caracteres de comando y y p. Coloque el cursor en el primer carácter que se seleccionará; luego, ingrese al modo visual. Use las teclas de flechas para expandir la selección visual. Cuando esté listo, presione y para extraer la selección en la memoria. Coloque el cursor en la nueva ubicación y, luego, presione p para *colocar* la selección en la posición del cursor.

Modo visual en Vim

El modo visual es útil para resaltar y manipular texto en diferentes líneas y columnas. Puede ingresar modos visuales en Vim usando las siguientes combinaciones de teclas.

- Modo de caracteres: **v**
- Modo de línea: **Shift+v**
- Modo de bloques: **Ctrl+v**

El modo de caracteres resalta oraciones en un bloque de texto. La palabra VISUAL aparece en la parte inferior de la pantalla. Presione v para entrar en el modo de caracteres visuales. Con Shift+v ingresa en el modo de líneas. En la parte inferior de la pantalla aparecerá VISUAL LINE.

El modo de bloques visuales es ideal para manipular archivos de datos. Presione la tecla Ctrl+v para ingresar al bloque visual desde el cursor. VISUAL BLOCK aparece en la parte inferior de la pantalla. Use las teclas de flecha para resaltar la sección que desea cambiar.

**nota**

Ser competente con el flujo de trabajo básico de Vim primero. Se necesita práctica para comprender las muchas capacidades de Vim. Familiarícese con esos conceptos básicos a través de la práctica y, luego, expanda su vocabulario de Vim aprendiendo más pulsaciones de teclas de Vim.

El ejercicio para esta sección usará el comando `vimtutor`. Este tutorial, de `vim-enhanced`, es una excelente manera de aprender las funciones centrales (core) de Vim.

Archivos de configuración de Vim

Los archivos de configuración `/etc/vimrc` y `~/.vimrc` alteran el comportamiento del editor `vim` para todo el sistema o un usuario específico, respectivamente. Dentro de estos archivos de configuración, puede especificar el comportamiento, como el espaciado de tabulación predeterminado, el resultado de sintaxis, los esquemas de color y más. La modificación del comportamiento del editor `vim` es particularmente útil cuando se trabaja con lenguajes como YAML, que tienen requisitos de sintaxis estrictos. Considere el siguiente archivo `~/.vimrc`, que establece la tabulación predeterminada (indicada por los caracteres `ts`) en dos espacios al editar archivos YAML. El archivo también incluye el parámetro `set number` para mostrar los números de línea mientras se editan todos los archivos.

```
[user@host ~]$ cat ~/.vimrc
autocmd FileType yaml setlocal ts=2
set number
```

Una lista completa de `vimrc` opciones de configuración está disponible en las referencias.

**Referencias**

Página del manual: `vim(1)`

El comando `:help` en `vim` (si el paquete `vim-enhanced` está instalado).

Manual de referencia de Vim: Opciones de Vim

<https://vimhelp.org/options.txt.html#options.txt>

► Ejercicio Guiado

Edición de archivos de texto desde el prompt de shell

En este ejercicio, usará el comando `vimtutor` para practicar técnicas básicas de edición en el editor `Vim`.

Resultados

- Editar archivos con Vim.
- Volverse más competente en el uso de Vim con el comando `vimtutor`.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start edit-editfile
```

Instrucciones

- 1. Use el comando `ssh` para iniciar sesión en la máquina `servera` con el usuario `student`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

- 2. Ejecute el comando `vimtutor`. Lea la pantalla de bienvenida y realice la Lección 1.1.

En la presentación, las teclas de flecha del teclado ayudan a navegar por la ventana. Inicialmente, cuando el editor `vi` se desarrolló por primera vez, los usuarios no podían confiar en tener teclas de flecha o asignaciones de teclado que funcionaran para que las teclas de flecha movieran el cursor. Por lo tanto, `vi` se diseñó originalmente para mover el cursor con comandos mediante las teclas de caracteres estándar, como las agrupadas convenientemente `h`, `j`, `k` y `l`.

A continuación se incluye una manera de recordarlas:

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

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

- 3. En la ventana `vimtutor`, realice la Lección 1.2.

En esta lección, se enseña a salir sin necesidad de conservar los cambios no deseados. Se pierden todos los cambios. A veces, es preferible perder los cambios antes que dejar un archivo vital en un estado incorrecto.

► **4.** En la ventana `vimtutor`, realice la *Lección 1.3*.

Vim ofrece pulsaciones de teclas rápidas y eficientes para eliminar una cantidad exacta de palabras, líneas, oraciones o párrafos. Cualquier edición es posible con la tecla `x` para la eliminación de un solo carácter.

► **5.** En la ventana `vimtutor`, realice la *Lección 1.4*.

Para la mayoría de las tareas de edición, la primera tecla que se presiona es la tecla `i`.

► **6.** En la ventana `vimtutor`, realice la *Lección 1.5*.

En la lección anterior, solo se enseñó el comando `i` (insertar) para ingresar al modo de edición. En esta lección, se demuestra el uso de otras teclas disponibles para cambiar la posición del cursor cuando se ingresa al modo de inserción. En el modo de inserción, todo el texto escrito cambia el contenido de archivo.

► **7.** En la ventana `vimtutor`, realice la *Lección 1.6*.

Escriba `:wq` para guardar el archivo y salir del editor.

► **8.** En la ventana `vimtutor`, lea el *Resumen de la Lección 1*.

El comando `vimtutor` incluye seis lecciones más de varios pasos. Estas lecciones no se asignan como parte de este curso, pero puede explorarlas para aprender más.

► **9.** Regrese al sistema `workstation` como el usuario `student`.

```
[student@servera ~]$ exit  
logout  
Connection to servera closed.  
[student@workstation ~]$
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish edit-editfile
```

Esto concluye la sección.

Configurar autenticación basada en claves de SSH

Objetivos

Configurar una cuenta de usuario para usar autenticación basada en claves para iniciar sesión en sistemas remotos de forma segura y sin una contraseña.

Autenticación basada en claves de SSH

Puede configurar su cuenta para el acceso sin contraseña a los servidores SSH que tienen habilitada la autenticación basada en claves, que se basa en el cifrado de clave pública (PKI).

Para preparar su cuenta, genere un par de archivos de claves relacionados criptográficamente. Una clave es privada y solo la tiene usted, mientras que la segunda es su clave pública relacionada que no es secreta. La clave privada actúa como su credencial de autenticación y debe almacenarse de forma segura. La clave pública se copia en su cuenta en servidores a los que accederá de forma remota, y verifica el uso de su clave privada.

Cuando inicia sesión en su cuenta en un servidor remoto, el servicio SSH usa su clave pública para verificar criptográficamente provista con la solicitud del cliente SSH. Si la verificación se realiza correctamente, su solicitud es de confianza y se le permite el acceso sin proporcionar una contraseña. Las contraseñas se pueden aprender o robar fácilmente, pero las claves privadas almacenadas de forma segura son más difíciles de comprometer.

Generación de claves SSH

Use el comando `ssh-keygen` para crear un par de claves. De manera predeterminada, el comando `ssh-keygen` guarda sus claves privadas y públicas en los archivos `~/.ssh/id_rsa` y `~/.ssh/id_rsa.pub`, pero puede especificar un nombre diferente.

```
[user@host ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/user/.ssh/id_rsa): Enter
Created directory '/home/user/.ssh'.
Enter passphrase (empty for no passphrase): Enter
Enter same passphrase again: Enter
Your identification has been saved in /home/user/.ssh/id_rsa.
Your public key has been saved in /home/user/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:vxutUNPi03QDCyvkYm1 user@host.lab.example.com
The key's randomart image is:
+---[RSA 2048]---+
|                               |
|                               |
|                               |
| . . . . |
| o o o o |
| . = o o . |
| o + = S E . |
| ..o o + * + |
| .+% 0 . + B . |
```

```
|=*o0 . . + *      |
|++. . +.      |
+---[SHA256]-----+
```

Puede elegir proporcionar una frase de contraseña a `ssh-keygen`, que se usa para cifrar su clave privada. Se recomienda usar una frase de contraseña, de modo que su clave privada no pueda ser usada por alguien que obtenga acceso a ella. Si establece una frase de contraseña, debe ingresar la frase de contraseña cada vez que use la clave privada. La frase de contraseña se usa localmente para descifrar su clave privada antes de usarla, a diferencia de su contraseña, que debe enviarse en texto sin cifrar a través de la red para su uso.

Puede usar el administrador de claves `ssh-agent` localmente, que almacena en caché su frase de contraseña al usarla por primera vez en una sesión de inicio de sesión, y luego proporciona la frase de contraseña para todos los usos posteriores de clave privada en la misma sesión de inicio de sesión. Este comando `ssh-agent` se analiza más adelante en esta sección.

En el siguiente ejemplo, se crea una clave privada protegida con frase de contraseña con la clave pública.

```
[user@host ~]$ ssh-keygen -f .ssh/key-with-pass
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase): your_passphrase
Enter same passphrase again: your_passphrase
Your identification has been saved in .ssh/key-with-pass.
Your public key has been saved in .ssh/key-with-pass.pub.
The key fingerprint is:
SHA256:w3GGB7EyHUr4a0cNPKmhNKS7dl1YsMVLvFZJ77VxAo user@host.lab.example.com
The key's randomart image is:
+---[RSA 2048]----+
|     . + =.o ... |
|     = B XEo o. |
|     . o O X =.... |
|     = = = B = o. |
|= + * * S .      |
| .+ = o + .      |
| + .              |
|                  |
|                  |
+---[SHA256]-----+
```

El comando `ssh-keygen` con la opción `-f` especifica los archivos en los que se guardarán las claves. En el ejemplo anterior, el comando `ssh-keygen` guardó el par de claves en los archivos `/home/user/.ssh/key-with-pass` y `/home/user/.ssh/key-with-pass.pub`.



Advertencia

Durante el uso del nuevo comando `ssh-keygen`, si especifica el nombre de un par de archivos de claves existente, incluido el par de claves predeterminado `id_rsa`, sobrescribirá ese par de claves existente, que solo se puede restaurar si tiene una copia de seguridad de esos archivos. Al sobrescribir un par de claves, se perderá la clave privada original que se requiere para acceder a las cuentas que ha configurado con el público correspondiente en los servidores remotos.

Si no puede restaurar su clave privada local, perderá el acceso a los servidores remotos hasta que distribuya su nueva clave pública para reemplazar la clave pública anterior en cada servidor. Cree siempre copias de seguridad de sus claves en caso de que se sobrescriban o se pierdan.

Una vez que se hayan generado las claves SSH, se guardarán de modo predeterminado en el directorio `.ssh` de su directorio de inicio. Para que funcione correctamente, el usuario privado deberá ser capaz de leerlo solo el propietario, que es un modo de permiso 600. Cualquier persona puede leer las claves públicas, lo que generalmente se establece como un modo de permiso 644.

Compartir la clave pública

Para configurar su cuenta remota para el acceso, copie su clave pública en el sistema remoto. El comando `ssh-copy-id` copia la clave pública del par de claves SSH en el sistema remoto. Puede especificar una clave pública específica con el comando `ssh-copy-id` o usar el archivo predeterminado `~/.ssh/id_rsa.pub`.

```
[user@host ~]$ ssh-copy-id -i .ssh/key-with-pass.pub user@remotehost
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/user/.ssh/
id_rsa.pub"
/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
user@remotehost's password: redhat
Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'user@remotehost'"
and check to make sure that only the key(s) you wanted were added.
```

Pruebe el acceso remoto, después de colocar la clave pública, con la clave privada correspondiente. Si la configuración es correcta, obtendrá acceso a su cuenta en el sistema remoto sin que se le solicite la contraseña de su cuenta. Si no especifica un archivo de clave privada, el comando `ssh` usa el archivo predeterminado `~/.ssh/id_rsa` si existe.



Importante

Si configuró una frase de contraseña para proteger su clave privada, SSH solicitará la frase de contraseña en el primer uso. Sin embargo, si la autenticación de la clave se realiza correctamente, no se le solicitará la contraseña de su cuenta.

```
[user@host ~]$ ssh -i .ssh/key-with-pass user@remotehost
Enter passphrase for key '.ssh/key-with-pass': your_passphrase
...output omitted...
[user@remotehost ~]$
```

Autenticación no interactiva con el administrador de claves

Si cifra su clave privada con una frase de contraseña, debe ingresar la frase de contraseña cada vez que use la clave privada para la autenticación. Sin embargo, puede configurar el administrador de claves **ssh-agent** para almacenar frases de contraseña en caché. Luego, cada vez que use SSH, el administrador de claves **ssh-agent** le proporcionará la frase de contraseña. El uso de un administrador de claves puede mejorar la seguridad al proporcionar menos oportunidades para que otras personas observen su frase de contraseña.

El administrador de claves **ssh-agent** se puede configurar para que se inicie automáticamente al iniciar sesión. El entorno de escritorio gráfico GNOME puede iniciar y configurar automáticamente el administrador de claves **ssh-agent**. Si inicia sesión en un entorno de texto, debe iniciar el programa **ssh-agent** manualmente para cada sesión. Inicie el programa **ssh-agent** con el siguiente comando:

```
[user@host ~]$ eval $(ssh-agent)
Agent pid 10155
```

Cuando inicia manualmente el comando **ssh-agent**, ejecuta comandos de shell adicionales para establecer variables de entorno que se necesitan para usar con el comando **ssh-add**. Puede cargar manualmente su frase de contraseña de clave privada en el administrador de claves con el comando **ssh-add**.

Los siguientes comandos de ejemplo **ssh-add** agregan las claves privadas del archivo `~/.ssh/id_rsa` predeterminado y después de un archivo `~/.ssh/key-with-pass`.

```
[user@host ~]$ ssh-add
Identity added: /home/user/.ssh/id_rsa (user@host.lab.example.com)
[user@host ~]$ ssh-add .ssh/key-with-pass
Enter passphrase for .ssh/key-with-pass: your_passphrase
Identity added: .ssh/key-with-pass (user@host.lab.example.com)
```

El siguiente comando **ssh** usa el archivo de clave privada predeterminado para acceder a su cuenta en un servidor SSH remoto.

```
[user@host ~]$ ssh user@remotehost
Last login: Mon Mar 14 06:51:36 2022 from host.example.com
[user@remotehost ~]$
```

El siguiente comando **ssh** usa el archivo de clave privada `~/.ssh/key-with-pass` para acceder a su cuenta en un servidor remoto. La clave privada en este ejemplo se descifró previamente y se agregó al administrador de claves **ssh-agent**, por lo que el comando **ssh** no le solicita la frase de contraseña para descifrar la clave privada.

```
[user@host ~]$ ssh -i .ssh/key-with-pass user@remotehost
Last login: Mon Mar 14 06:58:43 2022 from host.example.com
[user@remotehost ~]$
```

Cuando cierra sesión en una sesión que usó un administrador de claves `ssh-agent`, todas las frases de contraseña almacenadas en caché se borran de la memoria.

Solución de problemas básicos de conexión SSH

SSH puede parecer complejo cuando el acceso remoto mediante la autenticación de par de claves no se realiza correctamente. El comando `ssh` proporciona tres niveles de detalle con las opciones `-v`, `-vv` y `-vvv`, que proporcionan cantidades cada vez mayores de información de depuración durante el uso del comando `ssh`.

En el siguiente ejemplo, se demuestra la información provista cuando se usa la opción de nivel de detalle más baja:

```
[user@host ~]$ ssh -v user@remotehost
OpenSSH_8.7p1, OpenSSL 3.0.1 14 Dec 2021 ①
debug1: Reading configuration data /etc/ssh/ssh_config ②
debug1: Reading configuration data /etc/ssh/ssh_config.d/01-training.conf
debug1: /etc/ssh/ssh_config.d/01-training.conf line 1: Applying options for *
debug1: Reading configuration data /etc/ssh/ssh_config.d/50-redhat.conf
...output omitted...
debug1: Connecting to remotehost [192.168.1.10] port 22. ③
debug1: Connection established.
...output omitted...
debug1: Authenticating to remotehost:22 as 'user' ④
...output omitted...
debug1: Authentications that can continue: publickey,gssapi-keyex,gssapi-with-mic,password ⑤
...output omitted...
debug1: Next authentication method: publickey ⑥
debug1: Offering public key: /home/user/.ssh/id_rsa RSA
SHA256:hDVJjD7xrUjXGZVRJQixxFV6NF/ssMjS6AuQ1+VqUc4 ⑦
debug1: Server accepts key: /home/user/.ssh/id_rsa RSA
SHA256:hDVJjD7xrUjXGZVRJQixxFV6NF/ssMjS6AuQ1+VqUc4 ⑧
Authenticated to remotehost ([192.168.1.10]:22) using "publickey".
...output omitted...
[user@remotehost ~]$
```

- ① Versiones de OpenSSH y OpenSSL.
- ② Archivos de configuración OpenSSH.
- ③ Conexión al host remoto.
- ④ Métodos de autenticación que permite el host remoto.
- ⑤ Intentar autenticar al usuario en el host remoto.
- ⑥ Intentar autenticar al usuario con la clave SSH.
- ⑦ Uso del archivo de claves `/home/user/.ssh/id_rsa` para autenticar.

- ➊ Los hosts remotos aceptan la clave SSH.

Si un intento de método de autenticación falla, un servidor SSH remoto *fallará* a otros métodos de autenticación permitidos hasta que se prueben todos los métodos disponibles. En el siguiente ejemplo, se demuestra un acceso remoto con una clave SSH que falla, pero luego el servidor SSH ofrece autenticación de contraseña que se realiza correctamente.

```
[user@host ~]$ ssh -v user@remotehost
...output omitted...
debug1: Next authentication method: publickey
debug1: Offering public key: /home/user/.ssh/id_rsa RSA
SHA256:bsB6l5R184zvxNlrcRMmYd32oBkU1LgQj09dUBZ+Z/k
debug1: Authentications that can continue: publickey,gssapi-keyex,gssapi-with-mic,password
...output omitted...
debug1: Next authentication method: password
user@remotehost's password: password
Authenticated to remotehost ([172.25.250.10]:22) using "password".
...output omitted...
[user@remotehost ~]$
```

Configuración del cliente SSH

Puede crear el archivo `~/.ssh/config` para preconfigurar las conexiones SSH. Dentro del archivo de configuración, puede especificar parámetros de conexión, como usuarios, claves y puertos para hosts específicos. Este archivo elimina la necesidad de especificar manualmente los parámetros de los comandos cada vez que se conecta a un host. Considere el siguiente archivo `~/.ssh/config`, que preconfigura dos conexiones de host con diferentes usuarios y claves:

```
[user@host ~]$ cat ~/.ssh/config
host servera
  HostName          servera.example.com
  User              usera
  IdentityFile     ~/.ssh/id_rsa_servera

host serverb
  HostName          serverb.example.com
  User              userb
  IdentityFile     ~/.ssh/id_rsa_serverb
```

El archivo `~/.ssh/config` también es útil para configurar hosts de salto SSH. Un host de salto SSH es un servidor que actúa como un proxy para las conexiones SSH a otros hosts, generalmente internos. Considere un escenario en el que se puede acceder a un host llamado `external` a través de Internet, pero a un host llamado `internal` solo se puede acceder internamente. Use el parámetro `ProxyHost` dentro del archivo `~/.ssh/config` para conectarse al host `internal` a través del host `external`:

```
[user@host ~]$ cat ~/.ssh/config
host internal
    HostName           internal.example.com
    ProxyHost        external

host external
    HostName           external.example.com
```



Referencias

Páginas del manual: ssh-keygen(1), ssh-copy-id(1), ssh-agent(1) y ssh-add(1)

► Ejercicio Guiado

Configurar autenticación basada en claves de SSH

En este ejercicio, configura un usuario para realizar una autenticación basada en claves para SSH.

Resultados

- Generar un par de claves SSH sin protección de frase de contraseña.
- Generar un par de claves SSH con protección de frase de contraseña.
- Realizar la autenticación con claves SSH sin frase de contraseña y mediante claves SSH protegidas con frase de contraseña.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start ssh-configure
```

Instrucciones

- 1. Inicie sesión en la máquina `serverb` como el usuario `student`.

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
[student@serverb ~]$
```

- 2. Cambie al usuario `operator1` en la máquina `serverb`. Use `redhat` como la contraseña.

```
[student@serverb ~]$ su - operator1
Password: redhat
[operator1@serverb ~]$
```

- 3. Genere un conjunto de claves SSH. No ingrese una frase de contraseña.

```
[operator1@serverb ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/operator1/.ssh/id_rsa): Enter
Created directory '/home/operator1/.ssh'.
Enter passphrase (empty for no passphrase): Enter
Enter same passphrase again: Enter
Your identification has been saved in /home/operator1/.ssh/id_rsa.
```

```
Your public key has been saved in /home/operator1/.ssh/id_rsa.pub.  
The key fingerprint is:  
SHA256:JainiQdnRosC+xXh operator1@serverb.lab.example.com  
The key's randomart image is:  
+---[RSA 3072]---+  
|E+*+ooo . . . . |  
|.= 0.0 o . . . . |  
|o.. = . . o . . . |  
|+. + * . o . . . |  
|+ = X . S + . . . |  
| + @ + = . . . . |  
|. + = o . . . . . |  
| .o . . . . . . . |  
|o . . . . . . . . |  
+---[SHA256]---+
```

- ▶ 4. Envíe la clave pública del par de claves SSH al usuario **operator1** en la máquina **servera**, con **redhat** como contraseña.

```
[operator1@serverb ~]$ ssh-copy-id operator1@servera  
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/  
operator1/.ssh/id_rsa.pub"  
The authenticity of host 'servera (172.25.250.10)' can't be established.  
ED25519 key fingerprint is SHA256:h/hEJa/anxp6AP7BmB5azIPVbPNqieh0oKi4KWOTK80.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? 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  
operator1@servera's password: redhat  
  
Number of key(s) added: 1  
  
Now try logging into the machine, with: "ssh 'operator1@servera'"  
and check to make sure that only the key(s) you wanted were added.
```

- ▶ 5. Ejecute el comando **hostname** en la máquina **servera** de forma remota usando el comando **ssh** sin acceder a la shell interactiva remota.

```
[operator1@serverb ~]$ ssh operator1@servera hostname  
servera.lab.example.com
```

El comando **ssh** anterior no le solicitó una contraseña porque usó la clave privada sin frase de contraseña correspondiente a la clave pública exportada para realizar la autenticación como el usuario **operator1** en la máquina **servera**. Este enfoque no es seguro, ya que cualquier persona que tenga acceso al archivo de clave privada puede iniciar sesión en la máquina **servera** como el usuario **operator1**. La alternativa segura es proteger la clave privada con una frase de contraseña, lo cual se describe en un paso a continuación.

- ▶ 6. Genere otro conjunto de claves SSH con el nombre predeterminado y sin una frase de contraseña, sobrescribiendo los archivos de claves SSH generados anteriormente. Intente conectarse a la máquina **servera** con las nuevas claves SSH. El comando **ssh** solicita

una contraseña, ya que no puede autenticarse con la clave SSH. Ejecute nuevamente el comando `ssh` con la opción `-v` (detallado) para verificarlo.

Envíe la nueva clave pública del par de claves SSH al usuario `operator1` en la máquina `servera` para reemplazar la clave pública anterior. Use la contraseña `redhat` para el usuario `operator1` en la máquina `servera`. Ejecute el comando `hostname` en la máquina `servera` de forma remota usando el comando `ssh` sin acceder a la shell interactiva remota para comprobar que esté funcionando otra vez.

- 6.1. Nuevamente genere otro conjunto de claves SSH con el nombre predeterminado y sin una frase de contraseña, sobrescribiendo los archivos de claves SSH generados anteriormente.

```
[operator1@serverb ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/operator1/.ssh/id_rsa): Enter
/home/operator1/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase): Enter
Enter same passphrase again: Enter
Your identification has been saved in /home/operator1/.ssh/id_rsa
Your public key has been saved in /home/operator1/.ssh/id_rsa.pub
...output omitted...
```

- 6.2. Intente conectarse a la máquina `servera` con las nuevas claves SSH. El comando `ssh` solicita una contraseña, ya que no puede autenticarse con la clave SSH. Presione `Ctrl+c` para salir del comando `ssh` cuando se le solicite una contraseña. Ejecute nuevamente el comando `ssh` con la opción `-v` (detallado) para verificarlo. Presione `Ctrl+c` nuevamente para salir del comando `ssh` cuando se le solicite una contraseña.

```
[operator1@serverb ~]$ ssh operator1@servera hostname
operator1@servera's password: ^C
[operator1@serverb ~]$ ssh -v operator1@servera hostname
OpenSSH_8.7p1, OpenSSL 3.0.1 14 Dec 2021
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: Reading configuration data /etc/ssh/ssh_config.d/01-training.conf
...output omitted...
debug1: Next authentication method: publickey
debug1: Offering public key: /home/operator1/.ssh/id_rsa RSA
SHA256:ad597Zf64xckV26xht8bjQbzqSPuOXQPXksGEWVsP80
debug1: Authentications that can continue: publickey,gssapi-keyex,gssapi-with-mic,password
debug1: Trying private key: /home/operator1/.ssh/id_dsa
debug1: Trying private key: /home/operator1/.ssh/id_ecdsa
debug1: Trying private key: /home/operator1/.ssh/id_ecdsa_sk
debug1: Trying private key: /home/operator1/.ssh/id_ed25519
debug1: Trying private key: /home/operator1/.ssh/id_ed25519_sk
debug1: Trying private key: /home/operator1/.ssh/id_xmss
debug1: Next authentication method: password
operator1@servera's password: ^C
```

- 6.3. Envíe la nueva clave pública del par de claves SSH al usuario `operator1` en la máquina `servera` para reemplazar la clave pública anterior. Use la contraseña `redhat` para el usuario `operator1` en la máquina `servera`. Ejecute el comando

hostname en la máquina servera de forma remota usando el comando ssh sin acceder a la shell interactiva remota para comprobar que esté funcionando otra vez.

```
[operator1@serverb ~]$ ssh-copy-id operator1@servera
...output omitted...
operator1@servera's password: redhat

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'operator1@servera'"
and check to make sure that only the key(s) you wanted were added.
[operator1@serverb ~]$ ssh operator1@servera hostname
servera.lab.example.com
```

- ▶ 7. Genere otro conjunto de claves SSH protegidas con frase de contraseña. Guarde la clave como /home/operator1/.ssh/key2. Use redhatpass como la frase de contraseña de la clave privada.

```
[operator1@serverb ~]$ ssh-keygen -f .ssh/key2
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase): redhatpass
Enter same passphrase again: redhatpass
Your identification has been saved in .ssh/key2.
Your public key has been saved in .ssh/key2.pub.
The key fingerprint is:
SHA256:0CtCjfPm5QrbPBgqb operator1@serverb.lab.example.com
The key's randomart image is:
+---[RSA 3072]---+
|0=X*           |
|OB=.          |
|E*.o.         |
|Booo          |
|..= . o S     |
|+.o  o        |
|+.oo+ o       |
|+o.o.+        |
|+ . =o.       |
+---[SHA256]---
```

- ▶ 8. Envíe la clave pública del par de claves protegidas con frase de contraseña al usuario operator1 en la máquina servera. El comando no le solicitó una contraseña porque usó la clave pública de la clave privada sin frase de contraseña que exportó a la máquina servera en el paso anterior

```
[operator1@serverb ~]$ ssh-copy-id -i .ssh/key2.pub operator1@servera
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: ".ssh/key2.pub"
/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
```

```
Number of key(s) added: 1
```

Now try logging into the machine, with: "ssh 'operator1@servera'"
and check to make sure that only the key(s) you wanted were added.

- 9. Ejecute el comando `hostname` en la máquina `servera` de forma remota usando el comando `ssh`. Use la clave `/home/operator1/.ssh/key2` como el archivo de identidad. Ingrese la frase de contraseña `redhatpass` que definió para la clave privada en el paso anterior.

El comando le solicita la frase de contraseña que usó para proteger la clave privada del par de claves SSH. Si un atacante obtiene acceso a la clave privada, no podrá usarla para acceder a otros sistemas porque la clave privada está protegida con una frase de contraseña. El comando `ssh` usa una frase de contraseña diferente del usuario `operator1` en la máquina `servera`, por lo que los usuarios deben conocer ambas.

```
[operator1@serverb ~]$ ssh -i .ssh/key2 operator1@servera hostname
Enter passphrase for key '.ssh/key2': redhatpass
servera.lab.example.com
```

Puede usar el programa `ssh-agent`, como en el siguiente paso, para evitar escribir de forma interactiva la frase de contraseña al iniciar sesión con SSH. El uso del programa `ssh-agent` resulta más conveniente y más seguro cuando los administradores inician sesión en sistemas remotos con regularidad.

- 10. Ejecute el programa `ssh-agent` en la shell Bash y agregue la clave privada protegida con frase de contraseña (`/home/operator1/.ssh/key2`) del par de claves SSH a la sesión de shell.

El comando inicia el programa `ssh-agent` y configura esta sesión de shell para usarla. Luego, use el comando `ssh-add` para proporcionar la clave privada desbloqueada al programa `ssh-agent`.

```
[operator1@serverb ~]$ eval $(ssh-agent)
Agent pid 1729
[operator1@serverb ~]$ ssh-add .ssh/key2
Enter passphrase for .ssh/key2: redhatpass
Identity added: .ssh/key2 (operator1@serverb.lab.example.com)
```

- 11. Ejecute el comando `hostname` en la máquina `servera` de forma remota sin acceder a la shell interactiva remota. Use la clave `/home/operator1/.ssh/key2` como el archivo de identidad.

El comando no le solicita que ingrese la frase de contraseña de forma interactiva.

```
[operator1@serverb ~]$ ssh -i .ssh/key2 operator1@servera hostname
servera.lab.example.com
```

- 12. Abra otro terminal en la máquina `workstation` e inicie sesión en la máquina `serverb` como el usuario `student`.

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
[student@serverb ~]$
```

- 13. En la máquina **serverb**, cambie al usuario **operator1** e inicie sesión de forma remota en la máquina **servera**. Use la clave **/home/operator1/.ssh/key2** como el archivo de identidad para realizar la autenticación por medio de claves SSH.

- 13.1. Use el comando **su** para cambiar al usuario **operator1**. Use **redhat** como contraseña para el usuario **operator1**.

```
[student@serverb ~]$ su - operator1  
Password: redhat  
[operator1@serverb ~]$
```

- 13.2. Inicie sesión en la máquina **servera** como el usuario **operator1**.

El comando le solicita ingresar la frase de contraseña de manera interactiva porque no invoca la conexión SSH desde la misma shell que usó para iniciar el programa **ssh-agent**.

```
[operator1@serverb ~]$ ssh -i .ssh/key2 operator1@servera  
Enter passphrase for key '.ssh/key2': redhatpass  
...output omitted...  
[operator1@servera ~]$
```

- 14. Salga y cierre todos los terminales adicionales y regrese a la máquina **workstation**.

- 14.1. Salga y cierre las ventanas de terminal extra. El comando **exit** hizo que saliera de la shell del usuario **operator1**, finalizando la sesión de la shell donde **ssh-agent** estaba activo, y volviera a la shell del usuario **student** en la máquina **serverb**.

```
[operator1@servera ~]$ exit  
logout  
Connection to servera closed.  
[operator1@serverb ~]$
```

- 14.2. Regrese al sistema **workstation** como el usuario **student**.

```
[operator1@serverb ~]$ exit  
logout  
[student@serverb ~]$ exit  
logout  
Connection to serverb closed.  
[student@workstation ~]$
```

Finalizar

En la máquina **workstation**, cambie al directorio de inicio de usuario **student** y use el comando **lab** para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish ssh-configure
```

Esto concluye la sección.

Obtención de ayuda en el portal de clientes de Red Hat

Objetivos

Describir y usar los recursos clave en el portal de clientes de Red Hat para encontrar información en la documentación y la base de conocimientos de Red Hat.

Recursos del portal de clientes de Red Hat

El portal de clientes de Red Hat en <https://access.redhat.com> proporciona a los clientes acceso a documentación, descargas, herramientas y experiencia técnica. La base de conocimientos permite a los clientes buscar soluciones, preguntas frecuentes y artículos. En la siguiente lista, se muestran algunas funciones del Portal de clientes de Red Hat:

- Acceder a la documentación oficial de los productos, soluciones y preguntas frecuentes.
- Enviar y administrar casos de soporte.
- Gestionar las suscripciones y los derechos (entitlements) de software.
- Obtener descargas, actualizaciones y evaluaciones de software.
- Acceder a un catálogo de recomendaciones de seguridad para los productos de Red Hat.
- Acceda a un motor de búsqueda integrado para los recursos de Red Hat.
- Acceder a whitepapers, hojas de información y presentaciones multimedia.
- Participar en los debates de la comunidad.

Hay algunas secciones del sitio de acceso público y otras áreas están solo disponibles para clientes con suscripciones activas. Visite <https://access.redhat.com/help/> para obtener ayuda para acceder al Portal de clientes de Red Hat.

Recorrido del portal de clientes de Red Hat

Acceda al Portal de clientes de Red Hat visitando <https://access.redhat.com/>. Esta sección presenta el recorrido por el Portal de clientes de Red Hat en <https://access.redhat.com/start>.

Con el recorrido, puede descubrir las características del portal y aprovechar al máximo las ventajas de su suscripción a Red Hat. Una vez que haya iniciado sesión en el portal de clientes de Red Hat, haga clic en el botón **Tour the Customer Portal**.

Aparecerá la ventana **WELCOME TO THE RED HAT CUSTOMER PORTAL**. Haga clic en el botón **Let's go** para iniciar el recorrido.

Barra de navegación superior

Los primeros menús del recorrido, en la barra de navegación superior son Suscripciones, Descargas, Contenedores y Casos de soporte.

El menú **Subscriptions** abre una página nueva donde puede administrar los sistemas registrados y el uso de suscripciones y los derechos (entitlements). Esta página enumera la información de erratas aplicables. Puede crear claves de activación para registrar sistemas y garantizar los derechos (entitlements) correctos. El administrador de la organización de su cuenta puede restringir su acceso a esta página.

El menú **Downloads** abre una nueva página para acceder a las descargas de sus productos y solicitar la evaluación de los productos sin derechos (entitlements).

El menú **Support Cases** abre una página nueva que brinda acceso para crear, rastrear y administrar los casos de soporte a través del sistema de administración de casos, suponiendo que su organización ha autorizado ese nivel de acceso.

Con el menú **User Menu**, administre su cuenta, las cuentas de las que es administrador de la organización, su perfil y las opciones de notificación por correo electrónico.

El icono de globo terráqueo abre el menú **Language** para especificar sus preferencias de idioma para el portal de clientes de Red Hat.

Diríjase a los menús del Portal de clientes de Red Hat

Debajo de la barra de navegación superior en la página principal hay menús para navegar a las categorías principales de recursos disponibles en el sitio.

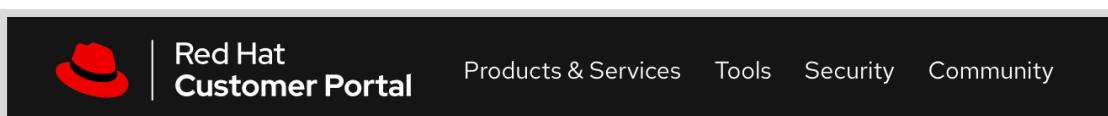


Figura 1.2: Menús del Portal de clientes de Red Hat

El menú **Products & Services** proporciona acceso a Product Hubs, que proporciona acceso a evaluaciones, resúmenes, guías de inicio y otra información de soporte específica para el producto. También puede acceder a la documentación sobre productos de Red Hat, a la base de conocimientos de artículos de soporte y cómo ponerse en contacto con el soporte de Red Hat. Puede acceder a los servicios que ofrece Red Hat, como consultoría, administración de cuentas técnicas y capacitación y certificaciones.

El menú **Tools** proporciona vínculos a herramientas para ayudarlo a tener éxito con los productos de Red Hat. Las herramientas ayudan a solucionar un problema de producto y proporcionan información de paquetes y erratas. La sección **Customer Portal Labs** proporciona una colección de aplicaciones y herramientas web para ayudarlo a mejorar el rendimiento, diagnosticar problemas, identificar problemas de seguridad y optimizar sus configuraciones. La sección **Red Hat Insights** ayuda a analizar plataformas y aplicaciones para predecir riesgos, tomar las medidas recomendadas y realizar un seguimiento de los costos para administrar entornos de nube híbrida. Insights alerta a los administradores antes de una interrupción, o sobre un evento de seguridad o un gasto excesivo.

El menú **Security** proporciona acceso al Centro de seguridad de productos de Red Hat para actualizaciones de seguridad y evita que los entornos se expongan a vulnerabilidades de seguridad. Esta sección proporciona información sobre problemas de seguridad de alto perfil, con acceso a las notificaciones de seguridad, la base de datos de *Vulnerabilidades y exposiciones comunes de Red Hat (CVE)*, los laboratorios de seguridad, el blog de seguridad de Red Hat, la medición de seguridad, las clasificaciones de gravedad, las políticas de backporting y las claves de firma de productos *GNU Privacy Guard (GPG)*.

El menú **Community** da acceso a la sección **Customer Portal Community** para debates y grupos privados. Esta sección permite que los expertos, clientes y partners de Red Hat se comuniquen y colaboren. Esta sección contiene foros de debate, blogs e información sobre los próximos eventos.

**nota**

Red Hat recomienda ver el recorrido completo en Iniciación con Red Hat [<https://access.redhat.com/start>], incluidas las secciones del menú **How to Personalize Your Customer Portal experience**, el menú **Explore the Benefits of Your Red Hat subscription** y el menú **How to Engage Red Hat Support**. Se requiere una suscripción activa para acceder a estos recursos de suscripción.

Póngase en contacto con el servicio de atención al cliente de Red Hat

El portal de clientes de Red Hat proporciona acceso a soporte técnico para clientes con una suscripción activa. Puede ponerse en contacto con soporte abriendo un caso de soporte o una sesión de chat, o por teléfono. Para obtener información detallada, visite la dirección https://access.redhat.com/support/policy/support_process.

Preparar un caso de soporte

Antes de comunicarse con la asistencia de Red Hat, es importante reunir la información relevante para el informe.

Defina el problema. Indique el problema y sus síntomas específicamente. Proporcione pasos detallados para reproducir el problema.

Reúna información básica. ¿Qué producto y versión se ven afectados? Esté preparado para brindar información de diagnóstico relevante. Esta información puede incluir la salida del comando `sos report`. 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 pila mostrado en el monitor de un sistema bloqueado.

Determine el nivel de gravedad. Red Hat usa cuatro niveles de gravedad para clasificar problemas. Los informes de problemas de gravedad *Urgente* y *Alta* debe seguirse mediante una llamada telefónica al centro de asistencia local pertinente (consulte <https://access.redhat.com/support/contact/technicalSupport>).

Gravedad	Descripción
Urgente (Gravedad 1)	Un problema que afecta gravemente su uso del software en un entorno de producción. Esta gravedad incluye la pérdida de datos de producción o el mal funcionamiento de los sistemas de producción. La situación interrumpe las operaciones empresariales y no existe un procedimiento de resolución.
Alta (Gravedad 2)	Un problema donde el software funciona, pero el uso en un entorno de producción se ve gravemente reducido. La situación tiene un gran impacto en sus operaciones empresariales y no existe un procedimiento de resolución.
Media (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, el problema implica un impacto medio a bajo en su empresa. La empresa sigue funcionando con una solución procesal. En entornos de desarrollo, la situación provoca problemas al migrar el proyecto a producción.

Gravedad	Descripción
Baja (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. En entornos de producción, el impacto en el negocio o en el rendimiento o la funcionalidad del sistema es bajo o inexistente. En entornos de desarrollo, el problema implica un impacto de medio a bajo en el negocio, pero la empresa continúa funcionando con un procedimiento de resolución.

Utilidad de informes SOS

El informe sos es generalmente el punto de partida para que el soporte técnico de Red Hat investigue el problema informado. Esta utilidad proporciona una manera estandarizada de recopilar información de diagnóstico que el soporte técnico de Red Hat necesita para investigar los problemas informados. El comando `sos report` recopila diversa información de depuración de uno o más sistemas y proporciona una opción para eliminar datos confidenciales. Este informe se adjunta al caso de soporte de Red Hat. El comando `sos collect` ejecuta y recopila informes sos individuales de un conjunto específico de nodos. El comando `sos clean` oculta información potencialmente confidencial, como nombres de usuario, nombres de host, direcciones IP o MAC u otros datos especificados por el usuario.

La siguiente lista contiene información que se puede recopilar en un informe:

- La versión del kernel en ejecución
- Módulos de kernel cargados
- Archivos de configuración del sistema y del servicio
- Salida del comando de diagnóstico
- Enumeración de todos los paquetes instalados

Generar el informe SOS

Red Hat Enterprise Linux instala la utilidad de informes sos con el paquete sos:

```
[root@host ~]# dnf install sos
...output omitted...
Complete!
```

La generación del informe sos requiere privilegios root. Ejecute el comando `sos report` para generar el informe.

```
[root@host ~]# sos report
...output omitted...
Press ENTER to continue, or CTRL-C to quit.

 Optionally, please enter the case id that you are generating this report for []:
...output omitted...
Your sosreport has been generated and saved in:
 /var/tmp/sosreport-host-2022-03-29-wixbhpz.tar.xz
...output omitted...
Please send this file to your support representative.
```

Cuando proporciona cualquier ID de caso de soporte en el comando anterior, el informe se adjunta directamente al caso de soporte creado anteriormente. También puede usar el comando `sos report` con la opción `--utility` para enviar el informe al soporte técnico.

Verifique que el comando `sos report` haya creado el archivo de almacenamiento en la ubicación anterior.

```
[root@host ~]# ls -l /var/tmp/
total 9388
-rw----- 1 root root 9605952 Mar 29 02:09 sosreport-host-2022-03-29-
wixbhpz.tar.xz
-rw-r--r-- 1 root root      65 Mar 29 02:09 sosreport-host-2022-03-29-
wixbhpz.tar.xz.sha256
...output omitted...
```

El comando `sos clean` oculta la información personal del informe.

```
[root@host ~]# sos clean /var/tmp/sosreport-host-2022-03-29-wixbhpz.tar.xz*
...output omitted...
Press ENTER to continue, or CTRL-C to quit.
...output omitted...
The obfuscated archive is available at
/var/tmp/sosreport-host0-2022-03-29-wixbhpz-obfuscated.tar.xz
...output omitted...
Please send the obfuscated archive to your support representative and keep the
mapping file private
```

Enviar el informe SOS al soporte técnico de Red Hat

Seleccione uno de estos métodos para enviar un informe `sos` al soporte técnico de Red Hat.

- Envíe el informe `sos` mediante el uso del comando `sos report` con la opción `--upload`.
- Envíe el informe `sos` al portal de clientes de Red Hat adjuntándolo al caso de soporte.

Únase al programa para desarrolladores de Red Hat

El programa para desarrolladores de Red Hat en <https://developers.redhat.com> proporciona derechos (entitlements) de suscripción al software de Red Hat para propósitos de desarrollo, documentación y libros de primera calidad de nuestros expertos en microservicios, computación sin servidor, Kubernetes y Linux. También hay disponibles enlaces de blogs a información sobre próximos eventos y capacitación, y otros recursos de ayuda.

Visite <https://developers.redhat.com/> para obtener más información.



Referencias

Página del manual: [sosreport\(1\)](#)

Contacto con la Asistencia técnica de Red Hat

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

Ayuda: Portal de clientes de Red Hat

<https://access.redhat.com/help/>

Para obtener más información, consulte *Generating an SOS Report for Technical Support* en

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/getting_the_most_from_your_support_experience/generating-an-sos-report-for-technical-support_getting-the-most-from-your-support-experience

► Ejercicio Guiado

Obtención de ayuda en el portal de clientes de Red Hat

En este ejercicio, genera un informe de diagnóstico mediante el uso de la consola web.

Resultados

- Generar un informe de diagnóstico con la consola web que podría enviarse al portal de clientes de Red Hat como parte de un caso de soporte.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start support-portal
```

Instrucciones

- 1. Inicie sesión en la máquina `servera` como el usuario `student`.

```
[student@workstation ~]$ ssh student@servera
Warning: Permanently added 'servera' (ED25519) to the list of known hosts.
Activate the web console with: systemctl enable --now cockpit.socket
...output omitted...
[student@servera ~]$
```

- 2. Inicie el servicio `cockpit`.

```
[student@servera ~]$ systemctl start cockpit.socket
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to start 'cockpit.socket'.
Authenticating as: Student User (student)
Password: student
==== AUTHENTICATION COMPLETE ====
[student@servera ~]$
```

- 3. Verifique el estado del servicio `cockpit`.

```
[student@servera ~]$ systemctl status cockpit.socket
● cockpit.socket - Cockpit Web Service Socket
   Loaded: loaded (/usr/lib/systemd/system/cockpit.socket; disabled; vendor
   preset: disabled)
     Active: active (listening) since Mon 2022-03-28 01:41:13 EDT; 1min 27s ago
```

```
Until: Mon 2022-03-28 01:41:13 EDT; 1min 27s ago
Triggers: • cockpit.service
Docs: man:cockpit-ws(8)
Listen: [::]:9090 (Stream)
...output omitted...
Mar 28 01:41:13 servera.lab.example.com systemd[1]: Starting Cockpit Web Service
Socket...
Mar 28 01:41:13 servera.lab.example.com systemd[1]: Listening on Cockpit Web
Service Socket.
```

► **4.** Regrese a la máquina **workstation** como el usuario **student**.

```
[student@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$
```

► **5.** En la máquina **workstation**, abra el navegador web Firefox e inicie sesión en la interfaz de la consola web que se ejecuta en la dirección **servera.lab.example.com**. Inicie sesión como el usuario **root** con la contraseña **redhat**.

- 5.1. Abra un navegador web Firefox y navegue a la dirección **https://servera.lab.example.com:9090**.
- 5.2. Cuando se le solicita, acepte el certificado autofirmado agregándolo como una excepción.
- 5.3. Inicie sesión como el usuario **root** con la contraseña **redhat**. Ya ha iniciado sesión como usuario privilegiado, lo cual es necesario para crear un informe de diagnóstico.
- 5.4. Haga clic en el menú **Diagnostic Reports** en el panel de navegación izquierdo. Haga clic en el botón **Create Report**. El informe tarda unos minutos en crearse.

► **6.** Cuando el informe esté listo, haga clic en el botón **Download report** para guardar el archivo.

- 6.1. Haga clic en el botón **Download report** y, luego, en **Save File**.
- 6.2. Cierre la sesión de la consola web y cierre el navegador web Firefox.

Finalizar

En la máquina **workstation**, cambie al directorio de inicio de usuario **student** y use el comando **lab** para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish support-portal
```

Esto concluye la sección.

Detección y resolución de problemas con Red Hat Insights

Objetivos

Usar Red Hat Insights para analizar los servidores en busca de problemas, corregirlos o resolverlos, y confirmar que la solución haya funcionado.

Presentación de Red Hat Insights

Red Hat Insights es una herramienta de análisis predictivo que ayuda a identificar y remediar las amenazas de seguridad, el rendimiento, la disponibilidad y la estabilidad de los sistemas en su infraestructura que ejecutan productos de Red Hat. Red Hat ofrece Red Hat Insights como un producto de software como servicio (SaaS), para que pueda implementarlo y escalarlo rápidamente sin requisitos de infraestructura adicionales. Además, puede aprovechar inmediatamente las últimas recomendaciones y actualizaciones de Red Hat que se aplican a los sistemas implementados.

Red Hat actualiza regularmente la base de conocimientos, sobre la base de los riesgos de soporte comunes, las vulnerabilidades de seguridad, las configuraciones erróneas conocidas y otros problemas identificados por Red Hat. Las acciones para mitigar o remediar estos problemas son validadas y verificadas por Red Hat. Con este soporte, puede identificar, priorizar y resolver proactivamente los problemas antes de que se conviertan en un problema mayor.

Para cada problema detectado, Red Hat Insights proporciona estimaciones del riesgo presentado y recomendaciones sobre cómo mitigar o remediar el problema. Estas recomendaciones pueden proporcionar materiales sugeridos, como Ansible Playbooks o instrucciones detalladas para ayudarle a resolver el problema.

Red Hat Insights adapta las recomendaciones a cada sistema registrado en el servicio. Para comenzar a usar Red Hat Insights, instale el agente que recopila metadatos sobre la configuración de tiempo de ejecución del sistema. Estos datos son un subconjunto de lo que podría proporcionar a Red Hat Support con el comando `sosreport` para resolver un ticket de soporte.

Puede limitar u ocultar los datos que envían sus sistemas cliente. Al limitar los datos, podría impedir el funcionamiento de algunas de las reglas analíticas, según lo que usted limite.

Después de registrar un servidor y de completar la sincronización inicial de metadatos del sistema, deberá ser capaz de ver su servidor y todas las recomendaciones para este en la consola de Insights en el portal de la nube de Red Hat.

Red Hat Insights actualmente proporciona análisis predictivos y recomendaciones para los siguientes productos de Red Hat:

- Red Hat Enterprise Linux 6.4 y versiones posteriores
- Red Hat Virtualization
- Red Hat Satellite 6 y versiones posteriores
- Red Hat OpenShift Container Platform
- Red Hat OpenStack Platform 7 y versiones posteriores
- Red Hat Ansible Automation Platform

Descripción de la arquitectura de Red Hat Insights

Cuando registra un sistema con Red Hat Insights, envía inmediatamente metadatos acerca de su configuración actual a la plataforma Red Hat Insights. Después del registro, el sistema actualiza periódicamente los metadatos provistos a Red Hat Insights. El sistema envía los metadatos con cifrado TLS para protegerlos en tránsito.

Cuando la plataforma de Red Hat Insights recibe los datos, los analiza y muestra el resultado en la consola web de Insights en el sitio <https://cloud.redhat.com/insights>.

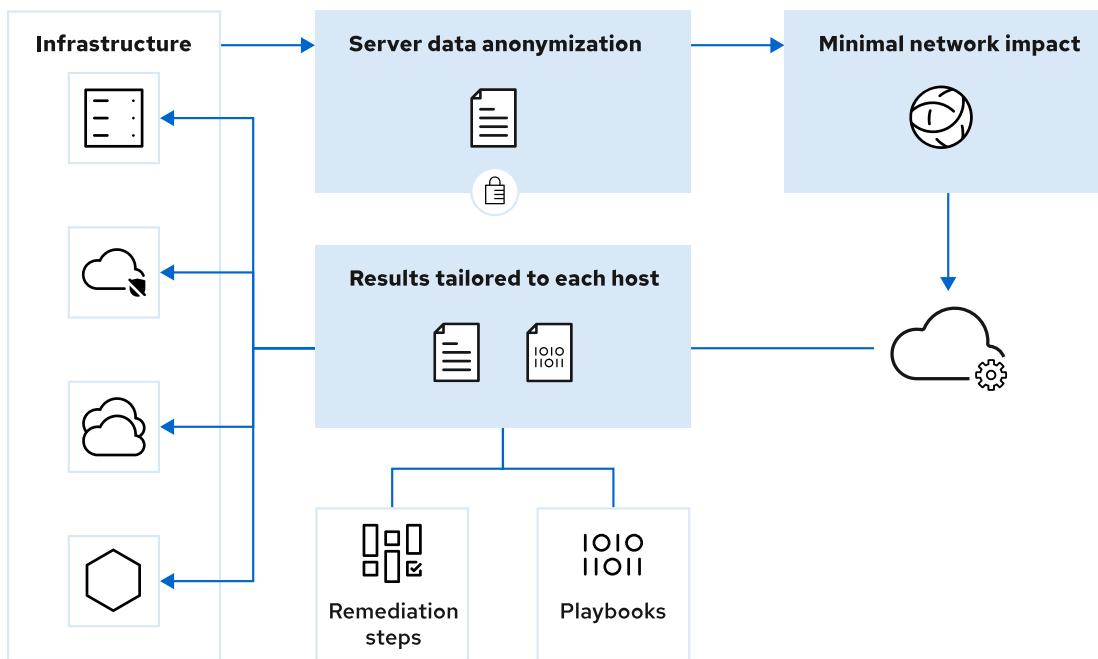


Figura 1.3: Arquitectura de alto nivel de Insights

Instalación de clientes de Red Hat Insights

Insights está incluido con Red Hat Enterprise Linux 9 como parte de la suscripción. Las versiones anteriores de los servidores de Red Hat Enterprise Linux requieren la instalación del paquete `insights-client` en el sistema. El paquete `insights-client` reemplaza el paquete `redhat-access-insights` que se inició con Red Hat Enterprise Linux 7.5.

Si registra su sistema para obtener derechos (entitlements) de software a través del servicio de administración de suscripciones del portal de clientes, puede activar Insights con un comando. Use el comando `insights-client --register` para registrar el sistema.

```
[root@host ~]# insights-client --register
```

El cliente de Insights actualiza periódicamente los metadatos que están proporcionados a Insights. Use el comando `insights-client` para actualizar los metadatos del cliente.

```
[root@host ~]# insights-client
Starting to collect Insights data for host.example.com
Uploading Insights data.
Successfully uploaded report for host.example.com.
View details about this system on cloud.redhat.com:
https://cloud.redhat.com/insights/inventory/dc480efd-4782-417e-a496-cb33e23642f0
```

Registro de un sistema de RHEL con Red Hat Insights

Registrar un servidor RHEL en Red Hat Insights es una tarea rápida.

Registre interactivamente el sistema con el servicio de Red Hat Subscription Management.

```
[root@host ~]# subscription-manager register --auto-attach
```

Asegúrese de que el paquete `insights-client` esté instalado en su sistema. El paquete se instala de forma predeterminada en RHEL 8 y sistemas posteriores.

```
[root@host ~]# dnf install insights-client
```

Use el comando `insights-client --register` para registrar el sistema con el servicio de Insights y cargar los metadatos iniciales del sistema.

```
[root@host ~]# insights-client --register
```

Confirme que el sistema esté visible en la sección **Inventory** en la consola web de Insights del sitio <https://cloud.redhat.com/insights>.

Name	Tags	OS	Last seen
serverb.lab.example.com		RHEL 9.1	Just now
servera.lab.example.com		RHEL 9.1	3 minutes ago
workstation.lab.example.com		RHEL 9.1	10 minutes ago

Figura 1.4: Inventario de Insights en el portal de nube

Navegación de la consola de Red Hat Insights

Insights proporciona una familia de servicios a los que accede a través de la consola web en el sitio <https://cloud.redhat.com/insights>.

Detección de problemas de configuración con el servicio de asesores

El servicio de asesores informa problemas de configuración que afectan sus sistemas. Puede acceder al servicio desde el menú **Advisor > Recommendations**.

Name	Added	Category	Total risk	Risk of change	Systems	Ansible
"SMBLoris" Samba denial of service with externally listening process	5 years ago	Security	Important	Very Low	1	Yes
Decreased security: Adobe Flash Player installed	6 months ago	Security	Moderate	Moderate	1	Yes
Decreased security: Yum GPG verification disabled (third-party repos)	4 years ago	Security	Important	Very Low	1	No
Traffic occurs or services are allowed unexpectedly when firewall zone drifting is enabled	2 years ago	Availability	Moderate	Moderate	1	No
Performance degradation of I/O when commands timeout due to faulty storage hardware	5 years ago	Stability	Important	Very Low	0	No
D-Bus timeout occurs when there are a large number of existing abrt crash directories	2 years ago	Availability	Moderate	Moderate	0	Yes
Asynchronous I/O related operations fall when kernel parameter fs.aio-max-nr limit is reached	3 years ago	Performance	Moderate	Low	0	No
Low density nodes detected	3 years ago	Performance	Moderate	Low	0	No
Running workload on nodes of an OpenShift cluster with an over-provisioned instance type size can result in cost increase	3 years ago	Performance	Moderate	Low	0	No

Figura 1.5: Recomendaciones del servicio de asesores

Para cada problema, Red Hat Insights proporciona información adicional para ayudarlo a comprender el problema, priorizar las tareas para resolverlo, determinar qué mitigación o corrección está disponible y automatizar su resolución con Ansible Playbook. Red Hat Insights también proporciona enlaces a artículos de la base de conocimiento en el Portal de clientes.

A denial of service flaw exists in Samba that allows a remote attacker to supply crafted NetBIOS Session Service headers and cause an out-of-memory state. A remote attacker in a position to supply the crafted data can render system unusable.

[Knowledgebase article](#)

[View the affected system](#)

Total risk
The total risk of this remediation is **important**, based on the combination of likelihood and impact to remediate.

Critical likelihood
High Impact

Risk of change
Very Low
The risk of change is **very low**, because the change takes very little time to implement and there is minimal impact to system operations.
 System reboot is **not required**.

Figura 1.6: Detalles de un problema

El servicio de asesores evalúa el riesgo de que se presente un problema en su sistema:

Riesgo total

Indica el impacto del problema en su sistema.

Riesgo de cambio

Indica el impacto de la acción de corrección en su sistema. Por ejemplo, es posible que deba reiniciar el sistema.

Evaluación de la seguridad con el servicio de vulnerabilidades

El servicio de vulnerabilidades informa las vulnerabilidades y exposiciones comunes (CVE) que afectan sus sistemas. Puede acceder al servicio desde el menú Vulnerability > CVEs.

Figura 1.7: Informe del servicio de vulnerabilidades

Para cada CVE, Insights proporciona información adicional y enumera los sistemas expuestos. Puede hacer clic en el botón **Remediate** para crear una Ansible Playbook para la corrección.

Figura 1.8: Detalles de un CVE

Análisis del cumplimiento mediante el servicio de cumplimiento

El servicio de cumplimiento analiza sus sistemas e informa su nivel de conformidad con una política de OpenSCAP. El proyecto OpenSCAP implementa herramientas para verificar la compatibilidad de un sistema con un conjunto de reglas. Red Hat Insights proporciona las reglas para evaluar sus sistemas con respecto a diferentes políticas, como el Norma de seguridad de datos del sector de tarjetas de pago (PCI DSS).

Actualización de paquetes con el servicio de parches

El servicio de parches enumera las recomendaciones de productos Red Hat que se aplican a sus sistemas. También puede generar una Ansible Playbook que puede ejecutar para actualizar los paquetes RPM asociados con los documentos aplicables. Para acceder a la lista de

recomendaciones para un sistema específico, use el menú **Patch > Systems**. Haga clic en el botón **Apply all applicable advisories** para generar Ansible Playbook para un sistema.

Name	Tags	OS	Packages	Applicable advisories	Last seen
workstation.lab.example.com		RHEL 9.1	2288	3 2 2	1 hour ago
servera.lab.example.com		RHEL 9.1	1278	No applicable advisories	Apply all applicable advisories
serverb.lab.example.com		RHEL 9.1	589	No applicable advisories	2 hours ago

Figura 1.9: Aplicación de parches a un sistema

Comparación de sistemas con el servicio de desajuste

Con el servicio de desajuste, puede comparar los sistemas u obtener un historial del sistema. Puede usar este servicio para solución de problemas, al comparar un sistema con otro sistema similar o con un estado anterior del sistema. Puede acceder al servicio desde el menú **Drift > Comparison**.

En la siguiente figura, se muestra que usted puede usar Red Hat Insights para comparar el mismo sistema en dos momentos diferentes:

Fact	State 1	State 2
arch	x86_64	x86_64
bios_release_date	04/01/2014	04/01/2014
bios_vendor	SeaBIOS	SeaBIOS
bios_version	1130-2-module+el8.2+7284+aa32a2c4	1130-2-module+el8.2+7284+aa32a2c4
cloud_provider		
cores_per_socket	1	1
cpu_flags		
cpu_model	Intel(R) Xeon(R) Gold 6248 CPU @ 250GHz	Intel(R) Xeon(R) Gold 6248 CPU @ 250GHz
enabled_services		
fqdn	workstation.lab.example.com	workstation.lab.example.com
infrastructure_type	virtual	virtual
infrastructure_vendor	kvm	kvm

Figura 1.10: Comparación de un historial del sistema

Activación de alertas con el servicio de políticas

Con el servicio de políticas, puede crear reglas para monitorear sus sistemas y enviar alertas cuando un sistema no cumple con las reglas. Red Hat Insights evalúa las reglas cada vez que un sistema sincroniza sus metadatos. Puede acceder al servicio desde el menú **Policies**.

The screenshot shows the Red Hat Hybrid Cloud Console interface. On the left, there's a sidebar with various navigation options like Dashboard, Advisor, Drift, Inventory, Vulnerability, Compliance, and Policies. The Policies option is currently selected. The main content area is titled 'Policies' and shows a table with one row. The row has a checkbox labeled '1 selected', a column for 'Name' containing 'No GCC', a 'Trigger actions' column with a bell icon, and a 'Last triggered' column showing 'Never'. Below the table, there's a 'Description' section stating 'Send a notification when the gcc package is installed.' and 'Last updated 28 Mar 2022 | Created 28 Mar 2022'. There's also a 'Conditions' section with the condition 'facts.installed_packages contains [gcc]' and a 'Trigger actions' section with the action 'Send a notification'.

Figura 1.11: Detalles de una regla personalizada

Guías de inventario y corrección, y monitoreo de suscripciones

En la página **Inventory**, se proporciona una lista de los sistemas que ha registrado con Red Hat Insights. En la columna **Last seen**, se muestra la hora de la actualización de metadatos más reciente para cada sistema. Al hacer clic en el nombre de un sistema, puede revisar sus detalles y acceder directamente a los servicios de asesor, vulnerabilidad, cumplimiento y parches para ese sistema.

En la página **Remediations** (Correcciones), se enumeran todas las Ansible Playbooks que creó para la corrección. Puede descargar las guías de esa página.

Mediante la página **Subscription**, puede monitorear su uso de la suscripción de Red Hat.



Referencias

Páginas del manual: `insights-client(8)` y `insights-client.conf(5)`

Para obtener más información acerca de Red Hat Insights, consulte la *Product Documentation for Red Hat Insights* en
https://access.redhat.com/documentation/en-us/red_hat_insights

Para obtener más información sobre la exclusión de datos recopilados por Insights, consulte los capítulos *Red Hat Insights Client Data Obfuscation* y *Red Hat Insights Client Data Redaction* en la *Client Configuration Guide for Red Hat Insights* en
https://access.redhat.com/documentation/en-us/red_hat_insights/2021/html-single/client_configuration_guide_for_red_hat_insights/assembly-main-client-cg

Hay información disponible sobre los datos recopilados por Red Hat Insights en
Información del sistema recopilada por Red Hat Insights
<https://access.redhat.com/articles/1598863>

► Cuestionario

Detección y resolución de problemas con Red Hat Insights

Elija las respuestas correctas para las siguientes preguntas:

► 1. ¿En qué orden ocurren los siguientes eventos cuando se administra un sistema de Red Hat Enterprise Linux con Red Hat Insights?

- 1) Red Hat Insights analyzes system metadata to determine which issues and recommendations apply.
 - 2) The Insights client uploads system metadata to the Red Hat Insights service.
 - 3) The administrator views the recommended actions in the Red Hat Insights customer portal.
 - 4) The Insights client collects system metadata on the Red Hat Enterprise Linux system.
-
- a. 1, 2, 3, 4
 - b. 4, 2, 1, 3
 - c. 4, 2, 3, 1
 - d. 4, 1, 2, 3

► 2. ¿Qué comando se usa para registrar un cliente en Red Hat Insights?

- a. insights-client --register
- b. insights-client --no-upload
- c. subscription-manager register
- d. insights-client --unregister

► 3. ¿Desde qué página de la consola de Red Hat Insights puede generar una Ansible Playbook para actualizar los paquetes RPM en un sistema?

- a. Advisor > Recommendations
- b. Vulnerability > Systems
- c. Patch > Systems
- d. Remediations

► Solución

Detección y resolución de problemas con Red Hat Insights

Elija las respuestas correctas para las siguientes preguntas:

► 1. ¿En qué orden ocurren los siguientes eventos cuando se administra un sistema de Red Hat Enterprise Linux con Red Hat Insights?

- 1) Red Hat Insights analyzes system metadata to determine which issues and recommendations apply.
 - 2) The Insights client uploads system metadata to the Red Hat Insights service.
 - 3) The administrator views the recommended actions in the Red Hat Insights customer portal.
 - 4) The Insights client collects system metadata on the Red Hat Enterprise Linux system.
-
- a. 1, 2, 3, 4
 - b. 4, 2, 1, 3
 - c. 4, 2, 3, 1
 - d. 4, 1, 2, 3

► 2. ¿Qué comando se usa para registrar un cliente en Red Hat Insights?

- a. insights-client --register
- b. insights-client --no-upload
- c. subscription-manager register
- d. insights-client --unregister

► 3. ¿Desde qué página de la consola de Red Hat Insights puede generar una Ansible Playbook para actualizar los paquetes RPM en un sistema?

- a. Advisor > Recommendations
- b. Vulnerability > Systems
- c. Patch > Systems
- d. Remediations

Resumen

- Puede usar el editor `vim` para crear y modificar archivos desde la línea de comandos.
- El comando `ssh-keygen` genera un par de claves SSH para la autenticación. El comando `ssh-copy-id` exporta la clave pública a sistemas remotos.
- Puede preconfigurar las conexiones SSH en el archivo de configuración `~/.ssh/config`.
- El portal de clientes de Red Hat brinda acceso a documentación, descargas, herramientas de optimización, administración de casos de soporte y administración de suscripciones y derechos (entitlements) para los productos de Red Hat.
- Red Hat Insights es una herramienta de análisis predictivo de SaaS que ayuda a identificar y corregir las amenazas a la seguridad, el rendimiento, la disponibilidad y la estabilidad de los sistemas.

capítulo 2

Administrar archivos desde la línea de comandos

Meta

Copiar, mover, crear, eliminar y organizar archivos desde la shell Bash.

Objetivos

- Describir cómo Linux organiza los archivos y los propósitos de diversos directorios en la jerarquía del sistema de archivos.
- Hacer que varios nombres de archivo hagan referencia al mismo archivo con enlaces duros y simbólicos (o "blandos").
- Ejecutar con eficiencia los comandos que afectan a muchos archivos mediante el uso de las funciones de coincidencia de patrones de la shell Bash.

Secciones

- Descripción de conceptos de la jerarquía del sistema de archivos Linux (y cuestionario)
- Creación de enlaces entre archivos (y ejercicio guiado)
- Coincidencia de nombres de archivo con expansiones de shell (y cuestionario)

Trabajo de laboratorio

- Administrar archivos desde la línea de comandos

Descripción de conceptos de la jerarquía del sistema de archivos Linux

Objetivos

Describir cómo Linux organiza los archivos y los propósitos de diversos directorios en la jerarquía del sistema de archivos.

La 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. Esta jerarquía es un árbol invertido porque se dice que la raíz del árbol está en la parte superior de la jerarquía, y las ramas de los directorios y subdirectorios se extienden debajo de la raíz.

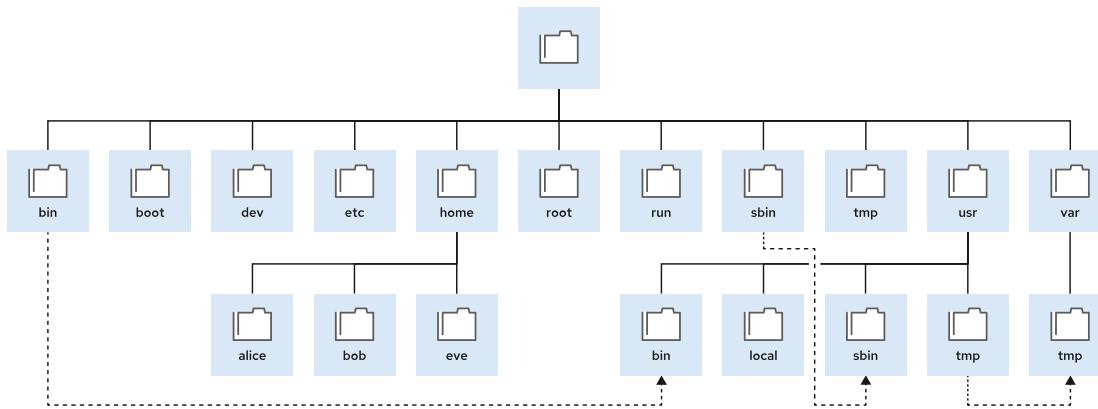


Figura 2.1: Directorios importantes del sistema de archivos de Red Hat Enterprise Linux 9

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

Los subdirectorios de / se usan con fines estandarizados para organizar archivos por tipo y objetivo, y hacer que sea más fácil encontrar los archivos. Por ejemplo, en el directorio root, el subdirectorio /boot se usa para guardar archivos para arrancar el sistema.

**nota**

Los siguientes términos ayudan a describir el contenido del directorio del sistema de archivos:

- El contenido *estático* no se modifica hasta que se edita o se reconfigura en forma explícita.
- El contenido *dinámico* o *variable* se puede modificar o adjuntar mediante procesos activos.
- El contenido *persistente* se mantiene después de un arranque nuevo, como los parámetros de configuración.
- El contenido de *tiempo de ejecución* de un proceso o del sistema se elimina al reiniciar.

En la siguiente tabla, se enumeran algunos de los directorios más importantes del sistema por nombre y objetivo.

Directarios importantes de Red Hat Enterprise Linux

Ubicación	Propósito
/boot	Archivos para iniciar el proceso de arranque.
/dev	Archivos de dispositivo especiales que el sistema usa para acceder al hardware.
/etc	Archivos de configuración específicos del sistema.
/home	Directorio de inicio, donde los usuarios habituales guardan sus datos y los archivos de configuración.
/root	Directorio de inicio para el superusuario administrativo, <code>root</code> .
/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. El contenido de este directorio se vuelve a crear en el arranque nuevo. Este directorio consolida los directorios /var/run y /var/lock de versiones anteriores de Red Hat Enterprise Linux.
/tmp	Un espacio con capacidad de escritura por parte de cualquier usuario del sistema 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. El directorio /var/tmp es también un directorio temporal, en el que los archivos que no tuvieron acceso, cambios ni modificaciones durante más de 30 días se eliminan automáticamente.
/usr	Software instalado, librerías compartidas, incluidos archivos y datos de programa de solo lectura. Los subdirectorios significativos incluyen: <ul style="list-style-type: none"> • /usr/bin: Comandos del usuario • /usr/sbin: Comandos de administración del sistema • /usr/local: Software personalizado a nivel local

Ubicación	Propósito
/var	Los datos variables específicos del sistema 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.

**Importante**

En Red Hat Enterprise Linux 7 y versiones posteriores, cuatro directorios antiguos en / 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 Red Hat Enterprise Linux 7 y versiones posteriores, los directorios de / son enlaces simbólicos a los directorios coincidentes de /usr.

**Referencias**

Página del manual: [hier\(7\)](#)

► Cuestionario

Descripción de conceptos de la jerarquía del sistema de archivos Linux

Elija las respuestas correctas para las siguientes preguntas:

- ▶ 1. **¿Qué directorio contiene datos de configuración persistentes y específicos del sistema?**
 - a. /etc
 - b. /root
 - c. /run
 - d. /usr

- ▶ 2. **¿Qué directorio está en la parte superior de la jerarquía del sistema de archivos del sistema?**
 - a. /etc
 - b. /
 - c. /home/root
 - d. /root

- ▶ 3. **¿Qué directorio contiene los directorios de inicio de los usuarios?**
 - a. /
 - b. /home
 - c. /root
 - d. /user

- ▶ 4. **¿Qué directorio contiene archivos para arrancar el sistema?**
 - a. /boot
 - b. /home/root
 - c. /bootable
 - d. /etc

- ▶ 5. **¿Qué directorio contiene archivos del sistema para acceder al hardware?**
 - a. /etc
 - b. /run
 - c. /dev
 - d. /usr

- ▶ 6. **¿Qué directorio es el directorio de inicio del superusuario administrativo?**
 - a. /etc
 - b. /
 - c. /home/root
 - d. /root
- ▶ 7. **¿Qué directorio contiene los comandos y las utilidades habituales?**
 - a. /commands
 - b. /run
 - c. /usr/bin
 - d. /usr/sbin
- ▶ 8. **¿Qué directorio contiene datos de tiempo de ejecución de procesos no persistentes?**
 - a. /tmp
 - b. /etc
 - c. /run
 - d. /var
- ▶ 9. **¿Qué directorio contiene las librerías y los programas de software instalados?**
 - a. /etc
 - b. /lib
 - c. /usr
 - d. /var

► Solución

Descripción de conceptos de la jerarquía del sistema de archivos Linux

Elija las respuestas correctas para las siguientes preguntas:

- ▶ 1. **¿Qué directorio contiene datos de configuración persistentes y específicos del sistema?**
 - a. /etc
 - b. /root
 - c. /run
 - d. /usr

- ▶ 2. **¿Qué directorio está en la parte superior de la jerarquía del sistema de archivos del sistema?**
 - a. /etc
 - b. /
 - c. /home/root
 - d. /root

- ▶ 3. **¿Qué directorio contiene los directorios de inicio de los usuarios?**
 - a. /
 - b. /home
 - c. /root
 - d. /user

- ▶ 4. **¿Qué directorio contiene archivos para arrancar el sistema?**
 - a. /boot
 - b. /home/root
 - c. /bootable
 - d. /etc

- ▶ 5. **¿Qué directorio contiene archivos del sistema para acceder al hardware?**
 - a. /etc
 - b. /run
 - c. /dev
 - d. /usr

- ▶ 6. **¿Qué directorio es el directorio de inicio del superusuario administrativo?**
 - a. /etc
 - b. /
 - c. /home/root
 - d. /root

- ▶ 7. **¿Qué directorio contiene los comandos y las utilidades habituales?**
 - a. /commands
 - b. /run
 - c. /usr/bin
 - d. /usr/sbin

- ▶ 8. **¿Qué directorio contiene datos de tiempo de ejecución de procesos no persistentes?**
 - a. /tmp
 - b. /etc
 - c. /run
 - d. /var

- ▶ 9. **¿Qué directorio contiene las librerías y los programas de software instalados?**
 - a. /etc
 - b. /lib
 - c. /usr
 - d. /var

Creación de enlaces entre archivos

Objetivos

Hacer que varios nombres de archivo hagan referencia al mismo archivo con enlaces duros y simbólicos (o "blandos").

Gestión de enlaces entre archivos

Puede crear varios nombres que apunten al mismo archivo. Estos nombres de archivos se denominan *enlaces*.

Puede crear dos tipos de enlaces: un *enlace duro* o un *enlace simbólico* (a veces denominado *enlace blando*). Cada forma tiene sus ventajas y desventajas.

Crear enlaces duros

Cada archivo comienza con un solo enlace duro, desde su nombre inicial hasta los datos en el sistema de archivos. Cuando crea un enlace duro a un archivo, crea otro nombre que apunta a esos mismos datos. El nuevo enlace duro actúa exactamente igual que el nombre del archivo original. Después de que se crea el enlace, no puede distinguir la diferencia entre el nuevo enlace duro y el nombre original del archivo.

Puede determinar si un archivo tiene varios enlaces duros mediante el comando `ls -l`. Un ítem que aparece es el *recuento de enlaces* de cada archivo, es decir, la cantidad de enlaces duros que tiene el archivo. En el ejemplo siguiente, el recuento de enlaces del archivo `newfile.txt` es 1. Tiene exactamente una ruta absoluta, que es la ubicación `/home/user/newfile.txt`.

```
[user@host ~]$ pwd
/home/user
[user@host ~]$ ls -l newfile.txt
-rw-r--r--. 1 user user 0 Mar 11 19:19 newfile.txt
```

Puede usar el comando `ln` para crear un enlace duro (otro nombre de archivo) que apunte a un archivo existente. El comando necesita al menos dos argumentos, una ruta al archivo existente y la ruta al enlace duro que desea crear.

En el siguiente ejemplo se crea un enlace duro llamado `newfile-hlink2.txt` con el nombre para el archivo existente `newfile.txt` en el directorio `/tmp`.

```
[user@host ~]$ ln newfile.txt /tmp/newfile-hlink2.txt
[user@host ~]$ ls -l newfile.txt /tmp/newfile-hlink2.txt
-rw-rw-r--. 2 user user 12 Mar 11 19:19 newfile.txt
-rw-rw-r--. 2 user user 12 Mar 11 19:19 /tmp/newfile-hlink2.txt
```

Para determinar si dos archivos tienen un enlace duro, use el comando `ls` con la opción `-i` para enumerar el *número de inodo* de cada archivo. Si los archivos están en el mismo sistema de archivos y sus números de inodo son los mismos, los archivos son enlaces duros que apuntan a los mismos contenidos de los archivos de datos.

```
[user@host ~]$ ls -il newfile.txt /tmp/newfile-hlink2.txt
8924107 -rw-rw-r--. 2 user user 12 Mar 11 19:19 newfile.txt
8924107 -rw-rw-r--. 2 user user 12 Mar 11 19:19 /tmp/newfile-hlink2.txt
```



Importante

Todos los enlaces duros que hacen referencia al mismo archivo tendrán la misma estructura de inodos con el recuento de enlaces, permiso de acceso, pertenencia a usuarios y grupos, marcas de tiempo y contenido de archivo. Cuando se cambia esa información para un enlace duro, los otros enlaces duros para el mismo archivo también muestran la nueva información. Esto se debe a que cada enlace duro apunta a los mismos datos en el dispositivo de almacenamiento.

Incluso si se elimina el archivo original, aún puede acceder al contenido del archivo siempre que exista al menos un enlace duro adicional. Los datos se eliminan del almacenamiento solo cuando se elimina el último enlace duro, lo que hace que el contenido del archivo no esté referenciado por ningún enlace duro.

```
[user@host ~]$ rm -f newfile.txt
[user@host ~]$ ls -l /tmp/newfile-hlink2.txt
-rw-rw-r--. 1 user user 12 Mar 11 19:19 /tmp/newfile-hlink2.txt
[user@host ~]$ cat /tmp/newfile-hlink2.txt
Hello World
```

Limitaciones de los enlaces duros

Los enlaces duros tienen algunas limitaciones. En primer lugar, los enlaces duros solo se pueden usar con archivos normales. No puede usar el comando `ln` para crear un enlace duro a un directorio o archivo especial.

En segundo lugar, solo puede usar enlaces duros si ambos archivos están en el mismo *sistema de archivos*. La jerarquía del sistema de archivos puede estar compuesta por varios dispositivos de almacenamiento. Dependiendo de la configuración de su sistema, cuando pase a un nuevo directorio, ese directorio y su contenido pueden almacenarse en un sistema de archivos diferente.

Puede usar el comando `df` para enumerar los directorios que están en diferentes sistemas de archivos. Por ejemplo, es posible que visualice la siguiente salida:

```
[user@host ~]$ df
Filesystem      1K-blocks   Used Available Use% Mounted on
devtmpfs          886788     0    886788  0% /dev
tmpfs            902108     0    902108  0% /dev/shm
tmpfs            902108   8696    893412  1% /run
tmpfs            902108     0    902108  0% /sys/fs/cgroup
/dev/mapper/rhel_rhel9--root 10258432 1630460   8627972 16% /
/dev/sda1        1038336 167128    871208 17% /boot
tmpfs           180420     0    180420  0% /run/user/1000
```

Los archivos que están en dos directorios diferentes con el indicador "Montado en" y sus subdirectorios están en sistemas de archivos distintos. Por lo tanto, en el sistema en este ejemplo, puede crear un enlace duro entre los archivos `/var/tmp/link1` y `/home/user/file` porque ambos son subdirectorios del directorio `/`, pero no de ningún otro directorio de la lista. Pero no

puede crear un enlace duro entre los archivos `/boot/test/badlink` y `/home/user/file` porque el primer archivo está en un subdirectorio del directorio `/boot` (en la lista "Montado en"), que se encuentra en el sistema de archivos `/dev/sda1`, en tanto que el segundo archivo está en el sistema de archivos `/dev/mapper/rhel_rhel9-root`.

Crear enlaces simbólicos

El comando `ln` con la opción `-s` crea un enlace simbólico, que también se conoce como "enlace blando". Un enlace simbólico no es un archivo regular, sino un tipo de archivo especial que apunta a un archivo o a un directorio existente.

Los enlaces simbólicos tienen algunas ventajas en comparación con los enlaces duros:

- Los enlaces simbólicos pueden vincular dos archivos en diferentes sistemas de archivos.
- Los enlaces simbólicos pueden apuntar a un directorio o archivo especial, no solo a un archivo regular.

En el siguiente ejemplo, el comando `ln -s` crea un enlace simbólico para el archivo `/home/user/newfile-link2.txt`. El nombre del enlace simbólico es `/tmp/newfile-symlink.txt`.

```
[user@host ~]$ ln -s /home/user/newfile-link2.txt /tmp/newfile-symlink.txt
[user@host ~]$ ls -l newfile-link2.txt /tmp/newfile-symlink.txt
-rw-rw-r--. 1 user user 12 Mar 11 19:19 newfile-link2.txt
lrwxrwxrwx. 1 user user 11 Mar 11 20:59 /tmp/newfile-symlink.txt -> /home/user/
newfile-link2.txt
[user@host ~]$ cat /tmp/newfile-symlink.txt
Symbolic Hello World
```

En el ejemplo anterior, el primer carácter de la lista larga para el archivo `/tmp/newfile-symlink.txt` es `l` (letra l) en lugar de `-`. Este carácter indica que el archivo es un enlace simbólico y no un archivo regular.

Cuando se elimina el archivo regular original, el enlace simbólico seguirá apuntando al archivo, pero el destino desaparece. Un enlace simbólico que apunta a un archivo que falta se denomina "enlace simbólico colgante".

```
[user@host ~]$ rm -f newfile-link2.txt
[user@host ~]$ ls -l /tmp/newfile-symlink.txt
lrwxrwxrwx. 1 user user 11 Mar 11 20:59 /tmp/newfile-symlink.txt -> /home/user/
newfile-link2.txt
[user@host ~]$ cat /tmp/newfile-symlink.txt
cat: /tmp/newfile-symlink.txt: No such file or directory
```



Importante

Un efecto secundario del enlace simbólico colgante en el ejemplo anterior es que si usted crea un archivo con el mismo nombre que el archivo eliminado (`/home/user/newfile-link2.txt`), el enlace simbólico ya no estará "colgando" y apuntará al archivo nuevo. Los enlaces duros no funcionan de esta forma. Si borra un enlace duro y luego usa herramientas normales (en lugar de `ln`) para crear un archivo con el mismo nombre, el nuevo archivo no se vincula al archivo anterior. Considere la siguiente manera de comparar enlaces duros y enlaces simbólicos para comprender cómo funcionan:

- Un enlace duro apunta un nombre a los datos de un dispositivo de almacenamiento.
- Un enlace simbólico apunta un nombre a otro nombre, que apunta a datos en un dispositivo de almacenamiento.

Un enlace simbólico puede apuntar a un directorio. El enlace simbólico funciona como un directorio. Si usa `cd` para cambiar al enlace simbólico, el directorio de trabajo actual se convierte en el directorio enlazado. Algunas herramientas pueden hacer un seguimiento del hecho de que usted siguió un enlace simbólico para llegar allí. Por ejemplo, de manera predeterminada, `cd` actualiza su directorio de trabajo actual por medio del nombre del enlace simbólico, y no del nombre del directorio real. Si desea actualizar el directorio de trabajo actual con el nombre del directorio real, puede usar la opción `-P`.

En el siguiente ejemplo, se crea un enlace simbólico llamado `/home/user/configfiles` que apunta al directorio `/etc`.

```
[user@host ~]$ ln -s /etc /home/user/configfiles
[user@host ~]$ cd /home/user/configfiles
[user@host configfiles]$ pwd
/home/user/configfiles
[user@host configfiles]$ cd -P /home/user/configfiles
[user@host etc]$ pwd
/etc
```



Referencias

Página del manual: `ln(1)`

`info ln (Make links between files)`

► Ejercicio Guiado

Creación de enlaces entre archivos

En este ejercicio, crea enlaces duros y enlaces simbólicos, y comparará los resultados.

Resultados

- Crear enlaces duros y enlaces simbólicos entre archivos.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start files-make
```

Instrucciones

- 1. Use el comando `ssh` para iniciar sesión en la máquina `servera` con el usuario `student`. La configuración del sistema admite el uso de claves SSH para la autenticación, por lo que no se necesita una contraseña.

```
[student@workstation ~]$ ssh student@servera  
...output omitted...  
[student@servera ~]$
```

- 2. Cree un enlace duro denominado `/home/student/links/file.hardlink` para el archivo `/home/student/files/target.file`. Verifique el recuento de enlaces para el archivo original y el nuevo archivo vinculado.

- 2.1. Vea el recuento de enlaces para el archivo `/home/student/files/target.file`.

```
[student@servera ~]$ ls -l files/target.file  
total 4  
-rw-r--r-- 1 student student 11 Mar 3 06:51 files/target.file
```

- 2.2. Cree un enlace duro denominado `/home/student/links/file.hardlink`. Establezca su enlace con el archivo `/home/student/files/target.file`.

```
[student@servera ~]$ ln /home/student/files/target.file \  
/home/student/links/file.hardlink
```

- 2.3. Verifique el recuento de enlaces para el archivo original `/home/student/files/target.file` y el nuevo archivo vinculado `/home/student/files/file.hardlink`. El recuento de enlaces debe ser de 2 para ambos archivos.

```
[student@servera ~]$ ls -l files/target.file links/file.hardlink
-rw-r--r--. 2 student student 11 Mar 3 06:51 files/target.file
-rw-r--r--. 2 student student 11 Mar 3 06:51 links/file.hardlink
```

- 3. Se crea un enlace simbólico llamado /home/student/tempdir que apunta al directorio /tmp en la máquina servera. Verifique el enlace simbólico recientemente creado.

- 3.1. Cree un enlace simbólico denominado /home/student/tempdir y vincúlelo al directorio /tmp.

```
[student@servera ~]$ ln -s /tmp /home/student/tempdir
```

- 3.2. Use el comando ls -l para verificar el enlace simbólico recién creado.

```
[student@servera ~]$ ls -l /home/student/tempdir
lrwxrwxrwx. 1 student student 4 Mar 3 06:55 /home/student/tempdir -> /tmp
```

- 4. Regrese al sistema workstation como el usuario student.

```
[student@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$
```

Finalizar

En la máquina workstation, cambie al directorio de inicio de usuario student y use el comando lab para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish files-make
```

Esto concluye la sección.

Coincidencia de nombres de archivo con expansiones de shell

Objetivos

Ejecutar con eficiencia los comandos que afectan a muchos archivos mediante el uso de las funciones de coincidencia de patrones de la shell Bash.

Expansiones de las líneas de comandos

La shell Bash tiene varias formas de expandir una línea de comandos, incluida la *coincidencia de patrones*, la expansión del directorio de inicio, la expansión de cadenas y la sustitución de variables. Quizás la más potente de estas maneras sea la de coincidencia de nombres de ruta, históricamente denominada *globbing*. Con la función de comodín de Bash, a veces denominada *comodines*, es más fácil administrar muchos archivos. Si se usan los *metacaracteres* que se "expanden" para establecer una coincidencia entre los archivos y los nombres de ruta que se buscan, los comandos actúan en un conjunto orientado de archivos de una vez.

Coincidencia de patrones

Globbing es una operación de análisis de comandos de la shell que expande un patrón de comodín en una lista de nombres de ruta coincidentes. Antes de la ejecución del comando, la shell reemplaza los metacaracteres de la línea de comando por la lista de coincidencias. Los patrones que no ofrecen coincidencias muestran la solicitud de patrón original como texto literal. En la siguiente tabla, se mencionan los metacaracteres y clases de patrones de uso frecuente.

Tabla de metacaracteres y coincidencias

Patrón	Coincidencias
*	Cualquier cadena de cero o más caracteres.
?	Cualquier carácter individual.
[abc...]	Cualquier carácter en la clase incluida (entre corchetes).
[!abc...]	Cualquier carácter que <i>no</i> esté en la clase incluida.
[^abc...]	Cualquier carácter que <i>no</i> esté en la clase incluida.
[:alpha:]	Cualquier carácter alfabético.
[:lower:]	Cualquier carácter en minúsculas.
[:upper:]	Cualquier carácter en mayúsculas.
[:alnum:]	Cualquier dígito o carácter alfabético.
[:punct:]	Cualquier carácter imprimible que no sea un espacio o alfanumérico.
[:digit:]	Cualquier dígito de 0 a 9.

Patrón	Coincidencias
<code>[:space:]</code>	Cualquier carácter de espacio en blanco, que puede incluir tabulaciones, nuevas líneas, retornos de carro, fuentes de formulario o espacios.

Para el siguiente ejemplo, simule que ha ejecutado los siguientes comandos para crear algunos archivos de muestra:

```
[user@host ~]$ mkdir glob; cd glob
[user@host glob]$ touch alpha bravo charlie delta echo able baker cast dog easy
[user@host glob]$ ls
able alpha baker bravo cast charlie delta dog easy echo
[user@host glob]$
```

En el siguiente ejemplo, los dos primeros comandos usan coincidencias de patrones simples con el asterisco (*) para hacer coincidir todos los nombres de archivos que comienzan con "a" y todos los nombres de archivos que contienen una "a", respectivamente. El tercer comando usa el asterisco y los corchetes para hacer coincidir todos los nombres de archivos que comienzan con "a" o "c".

```
[user@host glob]$ ls a*
able alpha
[user@host glob]$ ls *a*
able alpha baker bravo cast charlie delta easy
[user@host glob]$ ls [ac]*
able alpha cast charlie
```

En el siguiente ejemplo, también se usan caracteres de interrogación (?) para hacer coincidir algunos de esos nombres de archivo. Los dos comandos coinciden solo con nombres de archivos con cuatro y cinco caracteres de longitud, respectivamente.

```
[user@host glob]$ ls ****
able alpha cast easy echo
[user@host glob]$ ls ??????
baker bravo delta
```

Expansión de tilde

El carácter del tilde (~) coincide con el directorio de inicio del usuario actual. Si comienza con una cadena de caracteres que no tenga una barra (/), la shell interpreta que la cadena es un nombre de usuario hasta esa barra, si se logra una coincidencia, y reemplaza la cadena con la ruta absoluta al directorio de inicio de ese usuario. Si ningún nombre de usuario coincide, la shell empleará la propia tilde seguida de la cadena de caracteres.

En el siguiente ejemplo, el comando echo se usa para mostrar el valor del carácter de tilde. También puede usar el comando echo para mostrar los valores de los caracteres de expansión de llaves y variables, y otros.

```
[user@host glob]$ echo ~root
/root
[user@host glob]$ echo ~user
/home/user
[user@host glob]$ echo ~/glob
/home/user/glob
[user@host glob]$ echo ~nonexistinguser
~nonexistinguser
```

Expansión de llaves

La expansión de llaves se usa para generar cadenas discrecionales de caracteres. Las llaves contienen una lista de cadenas, o una expresión de cadenas, separadas por comas. El resultado incluye el texto que antecede o que sigue a la definición de llaves. Las expansiones de llaves pueden estar anidadas, una dentro de la otra. También puede usar la sintaxis de doble punto (...), que se expande a una secuencia. Por ejemplo, la sintaxis de doble punto {m..n} dentro de las llaves se expande a m n o p.

```
[user@host glob]$ echo {Sunday,Monday,Tuesday,Wednesday}.log
Sunday.log Monday.log Tuesday.log Wednesday.log
[user@host glob]$ echo file{1..3}.txt
file1.txt file2.txt file3.txt
[user@host glob]$ echo file{a..c}.txt
filea.txt fileb.txt filec.txt
[user@host glob]$ echo file{a,b}{1,2}.txt
filea1.txt filea2.txt fileb1.txt fileb2.txt
[user@host glob]$ echo file{a{1,2},b,c}.txt
filea1.txt filea2.txt fileb.txt filec.txt
```

La expansión de llaves se usa en la práctica, por ejemplo, para crear rápidamente múltiples archivos o directorios.

```
[user@host glob]$ mkdir ..../RHEL{7,8,9}
[user@host glob]$ ls ..../RHEL*
RHEL7 RHEL8 RHEL9
```

Expansión de variables

Una variable actúa como un contenedor con nombre que almacena un valor en la memoria. Las variables simplifican el acceso y la modificación de los datos almacenados desde la línea de comandos o dentro de un script de shell.

Puede asignar datos como valor de una variable con la siguiente sintaxis:

```
[user@host ~]$ VARIABLENAME=value
```

Puede usar la expansión de variables para convertir el nombre de la variable a su valor en la línea de comandos. Si una cadena comienza con un signo de dólar (\$), entonces la shell intentará usar el resto de esa cadena como un nombre de variable y reemplazarlo con un valor que tenga la variable.

```
[user@host ~]$ USERNAME=operator
[user@host ~]$ echo $USERNAME
operator
```

Para evitar errores debidos a otras expansiones de shell, puede poner el nombre de la variable entre llaves, por ejemplo, \${VARIABLENAME}.

```
[user@host ~]$ USERNAME=operator
[user@host ~]$ echo ${USERNAME}
operator
```

Los nombres de las variables solo pueden contener letras (mayúsculas y minúsculas), números y guiones bajos. Los nombres de las variables distinguen entre mayúsculas y minúsculas y no pueden comenzar con un número.

Sustitución de comandos

La sustitución de comandos permite obtener un comando para reemplazar el comando mismo en la línea de comandos. La sustitución de comandos se produce cuando un comando está entre paréntesis y precedido por un signo de dólar (\$). La forma \$(*command*) puede anidar varias expansiones de comando dentro de cada una.

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



nota

Una forma más antigua de sustitución de comandos usa acentos graves: `*command*` . Aunque la shell Bash aún acepta este formato, intente evitarlo porque es fácil confundir visualmente los acento grave con comillas simples, y los acento grave no se pueden anidar.

Cómo evitar la expansión de argumentos

Muchos caracteres tienen un significado especial en la shell Bash. Para evitar que la shell realice expansiones de shell en partes de su línea de comandos, puede usar caracteres y cadenas entre comillas y de escape.

La barra invertida (\) es un carácter de escape en la shell Bash. Evitará que el siguiente carácter se expanda.

```
[user@glob]$ echo The value of $HOME is your home directory.
The value of /home/user is your home directory.
[user@glob]$ echo The value of \$HOME is your home directory.
The value of $HOME is your home directory.
```

En el ejemplo anterior, con el signo de dólar protegido de la expansión, Bash lo trata como un carácter normal, sin la expansión de variables en \$HOME.

Para proteger las cadenas de caracteres más extensas, puede usar comillas simples (') o dobles ("") para encerrar las cadenas. Tienen efectos ligeramente diferentes. Las comillas simples detienen toda la expansión de shell. Las comillas dobles detienen la *mayor parte* de la expansión de shell.

Las comillas dobles suprimen el globbing y la expansión de la shell, pero permiten la sustitución de comandos y variables.

```
[user@host glob]$ myhost=$(hostname -s); echo $myhost
host
[user@host glob]$ echo "***** hostname is ${myhost} *****"
***** hostname is host *****
```

Use comillas simples para interpretar *todo* el texto literalmente.

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



Importante

Tanto en la pantalla como en el teclado, es fácil confundir la comilla simple (') y el acento grave de sustitución de comando (`). Si usa uno incorrectamente, cuando la intención era usar el otro, generará un comportamiento inesperado de la shell.



Referencias

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

► Cuestionario

Coincidencia de nombres de archivo con expansiones de shell

Elija las respuestas correctas para las siguientes preguntas:

- ▶ 1. ¿Qué patrón coincidirá solo con los nombres de archivo que terminan con "b"?
 - a. b*
 - b. *b
 - c. *b*
 - d. [!b] *

- ▶ 2. ¿Qué patrón coincidirá solo con los nombres de archivo que comienzan con "b"?
 - a. b*
 - b. *b
 - c. *b*
 - d. [!b] *

- ▶ 3. ¿Qué patrón coincidirá solo con los nombres de archivo donde el primer carácter no es "b"?
 - a. b*
 - b. *b
 - c. *b*
 - d. [!b] *

- ▶ 4. ¿Qué patrón coincidirá con todos los nombres de archivo que contienen "b"?
 - a. b*
 - b. *b
 - c. *b*
 - d. [!b] *

- ▶ 5. ¿Qué patrón coincidirá solo con los nombres de archivo que contienen un número?
 - a. *#*
 - b. *[:digit:]*
 - c. *[digit]*
 - d. [0-9]

- 6. ¿Qué patrón coincidirá solo con los nombres de archivo que comienzan con una letra mayúscula?
- a. ^?*
 - b. ^*
 - c. [upper]*
 - d. [:upper:]*
 - e. [[CAP]]*
- 7. ¿Qué patrón coincidirá solo con los nombres de archivo de al menos tres caracteres de longitud?
- a. ???*
 - b. ???
 - c. \3*
 - d. +++*
 - e. . . . *

► Solución

Coincidencia de nombres de archivo con expansiones de shell

Elija las respuestas correctas para las siguientes preguntas:

- ▶ 1. ¿Qué patrón coincidirá solo con los nombres de archivo que terminan con "b"?
 - a. b*
 - b. *b
 - c. *b*
 - d. [!b] *

- ▶ 2. ¿Qué patrón coincidirá solo con los nombres de archivo que comienzan con "b"?
 - a. b*
 - b. *b
 - c. *b*
 - d. [!b] *

- ▶ 3. ¿Qué patrón coincidirá solo con los nombres de archivo donde el primer carácter no es "b"?
 - a. b*
 - b. *b
 - c. *b*
 - d. [!b] *

- ▶ 4. ¿Qué patrón coincidirá con todos los nombres de archivo que contienen "b"?
 - a. b*
 - b. *b
 - c. *b*
 - d. [!b] *

- ▶ 5. ¿Qué patrón coincidirá solo con los nombres de archivo que contienen un número?
 - a. *#*
 - b. *[:digit:]*
 - c. *[digit]*
 - d. [0-9]

- 6. ¿Qué patrón coincidirá solo con los nombres de archivo que comienzan con una letra mayúscula?
- a. ^?*
 - b. ^*
 - c. [upper]*
 - d. [[:upper:]]*
 - e. [[CAP]]*
- 7. ¿Qué patrón coincidirá solo con los nombres de archivo de al menos tres caracteres de longitud?
- a. ???*
 - b. ???
 - c. \3*
 - d. +++*
 - e. . . . *

► Trabajo de laboratorio

Administrar archivos desde la línea de comandos

En este trabajo de laboratorio, crea, mueve y elimina archivos y directorios usando la shell y diversas técnicas de coincidencia de nombres de archivo.

Resultados

- Usar comodines para localizar y manipular archivos.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start files-review
```

Instrucciones

1. Use el comando `ssh` para iniciar sesión en la máquina `serverb` con el usuario `student`. La configuración del sistema admite el uso de claves SSH para la autenticación.
2. Cree un nuevo directorio llamado `project_plans` en el directorio `Documents`. El directorio `Documents` debe colocarse en el directorio de inicio del usuario `student`. Cree dos archivos vacíos en el directorio `project_plans` llamados `season1_project_plan.odf` y `season2_project_plan.odf`. Pista: Si el directorio `~/Documents` no existe, use el comando `mkdir` con la opción `-p` para crearlo.
3. Cree conjuntos de archivos de práctica vacíos para usar en este trabajo de laboratorio. Si no reconoce inmediatamente el atajo deseado de expansión de la shell, use la solución para aprender y practicar. Use la función de autocompletado con `tab` de la shell para localizar los nombres de ruta de archivos fácilmente. Cree 12 archivos con los nombres `tv_seasonX_episodeY.ogg` en el directorio `/home/student`. Reemplace `X` con el número de temporada e `Y` con el episodio de esa temporada, para dos temporadas de seis episodios cada una.
4. Como autor de una serie exitosa de novelas de misterio, está editando los capítulos de su próximo bestseller para publicarlos. Cree un total de ocho archivos con los nombres `mystery_chapterX.odf`. Reemplace la `X` con los números del 1 al 8.
5. Use un solo comando para crear dos subdirectorios llamados `season1` y `season2` en el directorio `Videos`, a fin de organizar los capítulos de la serie de televisión. Mueva los episodios de la serie de televisión correspondientes a los subdirectorios de temporadas. Use solo dos comandos y especifique los destinos con la sintaxis relativa.
6. Cree una jerarquía de directorios de dos niveles con un solo comando para organizar los capítulos del libro de misterios. Cree el subdirectorio `my_bestseller` en el directorio `Documents` y el subdirectorio `chapters` en el nuevo directorio `my_bestseller`. Cree tres

subdirectorios más directamente en el directorio `my_bestseller` con un solo comando. Nombre a estos subdirectorios `editor`, `changes` y `vacation`. No necesita usar el comando `mkdir -p` para crear elementos principales porque el directorio principal `my_bestseller` existe.

- Cambie al directorio `chapters`. Use el atajo del directorio de inicio con tilde (~) para mover todos los capítulos del libro al directorio `chapters`, que ahora es el directorio actual. Use la sintaxis más simple para especificar el directorio de destino.

Quiere enviar los primeros dos capítulos al editor para la revisión. Mueva solo esos dos capítulos al directorio `editor` para evitar modificarlos durante la revisión. Comenzando por el subdirectorio `chapters`, use la expansión de llaves con un rango para especificar los nombres de archivo de los capítulos que se moverán y una ruta relativa para el directorio de destino.

En las vacaciones, tiene la intención de escribir los capítulos 7 y 8. Use un solo comando para mover los archivos del directorio `chapters` al directorio `vacation`. Para especificar los nombres de archivo de los capítulos, use la expansión de llaves con una lista de cadenas y sin usar caracteres comodín.

- Cambie el directorio de trabajo a `~/Videos/season2` y copie el primer episodio de la temporada al directorio `vacation`. Use un solo comando `cd` para pasar del directorio de trabajo al directorio `~/Documents/my_bestseller/vacation`. Haga una lista de sus archivos. Use el argumento `directorio de trabajo anterior` para volver al directorio `season2`. (Este argumento se ejecutará correctamente si el último cambio de directorio con el comando `cd` se hizo con un comando en lugar de varios comandos `cd`). Desde el directorio `season2`, copie el archivo del episodio 2 en el directorio `vacation`. Use el atajo de nuevo para volver al directorio `vacation`.

- Los autores de los capítulos 5 y 6 quieren experimentar con posibles cambios. Copie ambos archivos del directorio `~/Documents/my_bestseller/chapters` al directorio `~/Documents/my_bestseller/changes` para evitar que estos cambios modifiquen los archivos originales. Diríjase al directorio `~/Documents/my_bestseller`. Use la coincidencia de patrones con corchetes para especificar qué números de capítulo deben coincidir en el argumento de nombre de archivo del comando `cp`.

- Cambie su directorio actual al directorio `changes` y use el comando `date +%F` con sustitución de comandos para copiar `mystery_chapter5.odf` a un archivo nuevo que incluya la fecha completa. Use el formato de nombre `mystery_chapter5_YYYY-MM-DD.odf`.

Al usar el reemplazo de comando con el comando `date +%s`, haga otra copia de `mystery_chapter5.odf` y anexe la marca de tiempo actual (como el número de segundos desde la era, 1-1-1970 00:00 UTC) para garantizar un nombre de archivo único.

- Después de una revisión adicional, usted decide que no necesita los cambios en la trama. Elimine el directorio `changes`.

De ser necesario, vaya al directorio `changes` y elimine todos los archivos del directorio. No puede eliminar un directorio mientras sea el directorio de trabajo actual.

Pase al directorio principal del directorio `changes`. Intente eliminar el directorio vacío con el comando `rm` sin la opción recursiva `-r`. Este intento debe fallar. Finalmente, use el comando `rmdir` para eliminar el directorio vacío; esta acción se ejecuta correctamente.

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

Una vez que haya finalizado, regrese al directorio de inicio del usuario `student`.

- Cree un enlace duro al archivo `~/Documents/project_plans/season2_project_plan.odf` denominado `~/Documents/backups/`

`season2_project_plan.odf.back`. Un enlace duro evita la eliminación accidental del archivo original y mantiene actualizado el archivo de respaldo a medida que cambia el original. Pista: Si el directorio `~/Documents/backups` no existe, use el comando `mkdir` para crearlo.

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade files-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish files-review
```

Esto concluye la sección.

► Solución

Administrar archivos desde la línea de comandos

En este trabajo de laboratorio, crea, mueve y elimina archivos y directorios usando la shell y diversas técnicas de coincidencia de nombres de archivo.

Resultados

- Usar comodines para localizar y manipular archivos.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start files-review
```

Instrucciones

1. Use el comando `ssh` para iniciar sesión en la máquina `serverb` con el usuario `student`. La configuración del sistema admite el uso de claves SSH para la autenticación.

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
```

2. Cree un nuevo directorio llamado `project_plans` en el directorio `Documents`. El directorio `Documents` debe colocarse en el directorio de inicio del usuario `student`. Cree dos archivos vacíos en el directorio `project_plans` llamados `season1_project_plan.odf` y `season2_project_plan.odf`. Pista: Si el directorio `~/Documents` no existe, use el comando `mkdir` con la opción `-p` para crearlo.

```
[student@serverb ~]$ mkdir -p ~/Documents/project_plans
[student@serverb ~]$ touch \
~/Documents/project_plans/{season1,season2}_project_plan.odf
[student@serverb ~]$ ls -lR Documents/
Documents:
total 0
drwxr-xr-x. 2 student student 70 Mar  7 03:50 project_plans

Documents/project_plans:
total 0
-rw-r--r--. 1 student student 0 Mar  7 03:50 season1_project_plan.odf
-rw-r--r--. 1 student student 0 Mar  7 03:50 season2_project_plan.odf
```

3. Cree conjuntos de archivos de práctica vacíos para usar en este trabajo de laboratorio. Si no reconoce inmediatamente el atajo deseado de expansión de la shell, use la solución para aprender y practicar. Use la función de autocompletado con tab de la shell para localizar los nombres de ruta de archivos fácilmente. Cree 12 archivos con los nombres `tv_seasonX_episodeY.ogg` en el directorio `/home/student`. Reemplace X con el número de temporada e Y con el episodio de esa temporada, para dos temporadas de seis episodios cada una.

```
[student@serverb ~]$ touch tv_season{1..2}_episode{1..6}.ogg
[student@serverb ~]$ ls tv*
tv_season1_episode1.ogg  tv_season1_episode5.ogg  tv_season2_episode3.ogg
tv_season1_episode2.ogg  tv_season1_episode6.ogg  tv_season2_episode4.ogg
tv_season1_episode3.ogg  tv_season2_episode1.ogg  tv_season2_episode5.ogg
tv_season1_episode4.ogg  tv_season2_episode2.ogg  tv_season2_episode6.ogg
```

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

```
[student@serverb ~]$ touch mystery_chapter{1..8}.odf
[student@serverb ~]$ ls mys*
mystery_chapter1.odf  mystery_chapter4.odf  mystery_chapter7.odf
mystery_chapter2.odf  mystery_chapter5.odf  mystery_chapter8.odf
mystery_chapter3.odf  mystery_chapter6.odf
```

5. Use un solo comando para crear dos subdirectorios llamados `season1` y `season2` en el directorio `Videos`, a fin de organizar los capítulos de la serie de televisión. Mueva los episodios de la serie de televisión correspondientes a los subdirectorios de temporadas. Use solo dos comandos y especifique los destinos con la sintaxis relativa.

- 5.1. Cree dos subdirectorios llamados `season1` y `season2` debajo del directorio `Videos` con un solo comando.

```
[student@serverb ~]$ mkdir -p Videos/season{1..2}
[student@serverb ~]$ ls Videos
season1  season2
```

- 5.2. Con tan solo dos comandos, mueva los episodios de la serie de televisión correspondientes a los subdirectorios de temporadas.

```
[student@serverb ~]$ mv tv_season1* Videos/season1
[student@serverb ~]$ mv tv_season2* Videos/season2
[student@serverb ~]$ ls -R Videos
Videos:
season1  season2

Videos/season1:
tv_season1_episode1.ogg  tv_season1_episode3.ogg  tv_season1_episode5.ogg
tv_season1_episode2.ogg  tv_season1_episode4.ogg  tv_season1_episode6.ogg

Videos/season2:
tv_season2_episode1.ogg  tv_season2_episode3.ogg  tv_season2_episode5.ogg
tv_season2_episode2.ogg  tv_season2_episode4.ogg  tv_season2_episode6.ogg
```

capítulo 2 | Administrar archivos desde la línea de comandos

6. Cree una jerarquía de directorios de dos niveles con un solo comando para organizar los capítulos del libro de misterios. Cree el subdirectorio `my_bestseller` en el directorio `Documents` y el subdirectorio `chapters` en el nuevo directorio `my_bestseller`. Cree tres subdirectorios más directamente en el directorio `my_bestseller` con un solo comando. Nombre a estos subdirectorios `editor`, `changes` y `vacation`. No necesita usar el comando `mkdir -p` para crear elementos principales porque el directorio principal `my_bestseller` existe.
- 6.1. Cree el directorio `my_bestseller` debajo del directorio `Documents`. Cree el directorio `chapters` debajo del directorio `my_bestseller`.

```
[student@serverb ~]$ mkdir -p Documents/my_bestseller/chapters
[student@serverb ~]$ ls -R Documents
Documents:
my_bestseller  project_plans

Documents/my_bestseller:
chapters

Documents/my_bestseller/chapters:

Documents/project_plans:
season1_project_plan.odf  season2_project_plan.odf
```

- 6.2. Cree tres directorios llamados `editor`, `changes` y `vacation` debajo del directorio `my_bestseller` con un solo comando.

```
[student@serverb ~]$ mkdir Documents/my_bestseller/{editor,changes,vacation}
[student@serverb ~]$ ls -R Documents
Documents:
my_bestseller  project_plans

Documents/my_bestseller:
changes  chapters  editor  vacation

Documents/my_bestseller/changes:

Documents/my_bestseller/chapters:

Documents/my_bestseller/editor:

Documents/my_bestseller/vacation:

Documents/project_plans:
season1_project_plan.odf  season2_project_plan.odf
```

7. Cambie al directorio `chapters`. Use el atajo del directorio de inicio con tilde (~) para mover todos los capítulos del libro al directorio `chapters`, que ahora es el directorio actual. Use la sintaxis más simple para especificar el directorio de destino.

Quiere enviar los primeros dos capítulos al editor para la revisión. Mueva solo esos dos capítulos al directorio `editor` para evitar modificarlos durante la revisión. Comenzando por el subdirectorio `chapters`, use la expansión de llaves con un rango para especificar los nombres de archivo de los capítulos que se moverán y una ruta relativa para el directorio de destino.

capítulo 2 | Administrar archivos desde la línea de comandos

En las vacaciones, tiene la intención de escribir los capítulos 7 y 8. Use un solo comando para mover los archivos del directorio **chapters** al directorio **vacation**. Para especificar los nombres de archivo de los capítulos, use la expansión de llaves con una lista de cadenas y sin usar caracteres comodín.

- 7.1. Cambie al directorio **chapters** y use el atajo del directorio de inicio con tilde (~) para mover todos los capítulos del libro al directorio **chapters**.

```
[student@serverb ~]$ cd Documents/my_bestseller/chapters
[student@serverb chapters]$ mv ~/mystery_chapter* .
[student@serverb chapters]$ ls
mystery_chapter1.odf mystery_chapter4.odf mystery_chapter7.odf
mystery_chapter2.odf mystery_chapter5.odf mystery_chapter8.odf
mystery_chapter3.odf mystery_chapter6.odf
```

- 7.2. Mueva los dos primeros capítulos al directorio **editor**. Use la expansión de llaves con un rango para especificar los nombres de archivo de los capítulos que se moverán y una ruta relativa para el directorio de destino.

```
[student@serverb chapters]$ mv mystery_chapter{1..2}.odf ../editor
[student@serverb chapters]$ ls
mystery_chapter3.odf mystery_chapter5.odf mystery_chapter7.odf
mystery_chapter4.odf mystery_chapter6.odf mystery_chapter8.odf
[student@serverb chapters]$ ls ../editor
mystery_chapter1.odf mystery_chapter2.odf
```

- 7.3. Use un solo comando para mover los capítulos 7 y 8 del directorio **chapters** al directorio **vacation**. Para especificar los nombres de archivo de los capítulos, use la expansión de llaves con una lista de cadenas y sin usar caracteres comodín.

```
[student@serverb chapters]$ mv mystery_chapter{7,8}.odf ../vacation
[student@serverb chapters]$ ls
mystery_chapter3.odf mystery_chapter5.odf
mystery_chapter4.odf mystery_chapter6.odf
[student@serverb chapters]$ ls ../vacation
mystery_chapter7.odf mystery_chapter8.odf
```

8. Cambie el directorio de trabajo a **~/Videos/season2** y copie el primer episodio de la temporada al directorio **vacation**. Use un solo comando **cd** para pasar del directorio de trabajo al directorio **~/Documents/my_bestseller/vacation**. Haga una lista de sus archivos. Use el argumento *directorio de trabajo anterior* para volver al directorio **season2**. (Este argumento se ejecutará correctamente si el último cambio de directorio con el comando **cd** se hizo con un comando en lugar de varios comandos **cd**). Desde el directorio **season2**, copie el archivo del episodio 2 en el directorio **vacation**. Use el atajo de nuevo para volver al directorio **vacation**.

- 8.1. Cambie el directorio de trabajo a **~/Videos/season2** y copie el primer episodio de la temporada al directorio **vacation**.

```
[student@serverb chapters]$ cd ~/Videos/season2
[student@serverb season2]$ cp *episode1.ogg ~/Documents/my_bestseller/vacation
```

capítulo 2 | Administrar archivos desde la línea de comandos

- 8.2. Use un solo comando cd para cambiar de su directorio de trabajo al directorio ~/Documents/my_bestseller/vacation, enumere sus archivos y use el argumento - para regresar al directorio anterior. Copie el archivo del episodio 2 en el directorio vacation. Use el comando cd con el argumento - para regresar al directorio vacation.

```
[student@serverb season2]$ cd ~/Documents/my_bestseller/vacation
[student@serverb vacation]$ ls
mystery_chapter7.odf mystery_chapter8.odf tv_season2_episode1.ogg
[student@serverb vacation]$ cd -
/home/student/Videos/season2
[student@serverb season2]$ cp *episode2.ogg ~/Documents/my_bestseller/vacation
[student@serverb season2]$ cd -
/home/student/Documents/my_bestseller/vacation
[student@serverb vacation]$ ls
mystery_chapter7.odf tv_season2_episode1.ogg
mystery_chapter8.odf tv_season2_episode2.ogg
```

9. Los autores de los capítulos 5 y 6 quieren experimentar con posibles cambios. Copie ambos archivos del directorio ~/Documents/my_bestseller/chapters al directorio ~/Documents/my_bestseller/changes para evitar que estos cambios modifiquen los archivos originales. Diríjase al directorio ~/Documents/my_bestseller. Use la coincidencia de patrones con corchetes para especificar qué números de capítulo deben coincidir en el argumento de nombre de archivo del comando cp.

```
[student@serverb vacation]$ cd ~/Documents/my_bestseller
[student@serverb my_bestseller]$ cp chapters/mystery_chapter[56].odf changes
[student@serverb my_bestseller]$ ls chapters
mystery_chapter3.odf mystery_chapter5.odf
mystery_chapter4.odf mystery_chapter6.odf
[student@serverb my_bestseller]$ ls changes
mystery_chapter5.odf mystery_chapter6.odf
```

10. Cambie su directorio actual al directorio changes y use el comando date +%F con sustitución de comandos para copiar mystery_chapter5.odf a un archivo nuevo que incluya la fecha completa. Use el formato de nombre mystery_chapter5_YYYY-MM-DD.odf.

Al usar el reemplazo de comando con el comando date +%s, haga otra copia de mystery_chapter5.odf y anexe la marca de tiempo actual (como el número de segundos desde la era, 1-1-1970 00:00 UTC) para garantizar un nombre de archivo único.

```
[student@serverb my_bestseller]$ cd changes
[student@serverb changes]$ cp mystery_chapter5.odf \
mystery_chapter5_$(date +%F).odf
[student@serverb changes]$ cp mystery_chapter5.odf \
mystery_chapter5_$(date +%s).odf
[student@serverb changes]$ ls
mystery_chapter5_1646644424.odf mystery_chapter5.odf
mystery_chapter5_2022-03-07.odf mystery_chapter6.odf
```

11. Después de una revisión adicional, usted decide que no necesita los cambios en la trama. Elimine el directorio changes.

capítulo 2 | Administrar archivos desde la línea de comandos

De ser necesario, vaya al directorio `changes` y elimine todos los archivos del directorio. No puede eliminar un directorio mientras sea el directorio de trabajo actual.

Pase al directorio principal del directorio `changes`. Intente eliminar el directorio vacío con el comando `rm` sin la opción recursiva `-r`. Este intento debe fallar. Finalmente, use el comando `rmdir` para eliminar el directorio vacío; esta acción se ejecuta correctamente.

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

Una vez que haya finalizado, regrese al directorio de inicio del usuario `student`.

- 11.1. Elimine el directorio `changes`. Cambie al directorio padre del directorio `changes` e intente eliminar el directorio vacío usando el comando `rm` sin la opción recursiva `-r`, que debería fallar. Use el comando `rmdir` para eliminar el directorio vacío.

```
[student@serverb changes]$ rm mystery*
[student@serverb changes]$ cd ..
[student@serverb my_bestseller]$ rm changes
rm: cannot remove 'changes': Is a directory
[student@serverb my_bestseller]$ rmdir changes
[student@serverb my_bestseller]$ ls
chapters editor vacation
```

- 11.2. Elimine el directorio `vacation` usando el comando `rm` con la opción `-r`. Regrese al directorio de inicio del usuario `student`.

```
[student@serverb my_bestseller]$ rm -r vacation
[student@serverb my_bestseller]$ ls
chapters editor
[student@serverb my_bestseller]$ cd
[student@serverb ~]$
```

12. Cree un enlace duro al archivo `~/Documents/project_plans/season2_project_plan.odf` denominado `~/Documents/backups/season2_project_plan.odf.back`. Un enlace duro evita la eliminación accidental del archivo original y mantiene actualizado el archivo de respaldo a medida que cambia el original. Pista: Si el directorio `~/Documents/backups` no existe, use el comando `mkdir` para crearlo.

- 12.1. Cree un enlace duro al archivo `~/Documents/project_plans/season2_project_plan.odf` denominado `~/Documents/backups/season2_project_plan.odf.back`.

```
[student@serverb ~]$ mkdir ~/Documents/backups
[student@serverb ~]$ ln ~/Documents/project_plans/season2_project_plan.odf \
~/Documents/backups/season2_project_plan.odf.back
[student@serverb ~]$ ls -lR ~/Documents/
/home/student/Documents/:
total 0
drwxr-xr-x. 2 student student 43 Mar  7 04:18 backups
drwxr-xr-x. 4 student student 36 Mar  7 04:16 my_bestseller
drwxr-xr-x. 2 student student 70 Mar  7 03:50 project_plans

/home/student/Documents/backups:
```

capítulo 2 | Administrar archivos desde la línea de comandos

```
total 0
-rw-r--r--. 2 student student 0 Mar  7 03:50 season2_project_plan.odf.back

/home/student/Documents/my_bestseller:
total 0
drwxr-xr-x. 2 student student 118 Mar  7 04:07 chapters
drwxr-xr-x. 2 student student  62 Mar  7 04:06 editor

/home/student/Documents/my_bestseller/chapters:
total 0
-rw-r--r--. 1 student student 0 Mar  7 03:56 mystery_chapter3.odf
-rw-r--r--. 1 student student 0 Mar  7 03:56 mystery_chapter4.odf
-rw-r--r--. 1 student student 0 Mar  7 03:56 mystery_chapter5.odf
-rw-r--r--. 1 student student 0 Mar  7 03:56 mystery_chapter6.odf

/home/student/Documents/my_bestseller/editor:
total 0
-rw-r--r--. 1 student student 0 Mar  7 03:56 mystery_chapter1.odf
-rw-r--r--. 1 student student 0 Mar  7 03:56 mystery_chapter2.odf

/home/student/Documents/project_plans:
total 0
-rw-r--r--. 1 student student 0 Mar  7 03:50 season1_project_plan.odf
-rw-r--r--. 2 student student 0 Mar  7 03:50 season2_project_plan.odf
```

Tenga en cuenta que el recuento de enlaces es 2 para los archivos `season2_project_plan.odf.back` y `season2_project_plan.odf`.

12.2. Regrese al sistema `workstation` como el usuario `student`.

```
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@workstation ~]$
```

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade files-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish files-review
```

Esto concluye la sección.

Resumen

- Los archivos de un sistema Linux se organizan en un árbol de directorios invertido individual, una jerarquía de sistema de archivos.
- Los enlaces duros y los enlaces blandos son formas diferentes de hacer que varios nombres de archivo apunten a los mismos datos.
- La shell Bash ofrece funciones de coincidencia de patrones, expansión y sustitución para ayudarlo a ejecutar los comandos de manera eficiente.

capítulo 3

Administración de usuarios y grupos locales

Meta

Crear, administrar y eliminar usuarios y grupos locales, y administrar políticas de contraseña locales.

Objetivos

- Describir el propósito de los usuarios y grupos en un sistema Linux.
- Cambiar a la cuenta de superusuario para administrar un sistema Linux y otorgar a otros usuarios acceso de superusuario a través del comando `sudo`.
- Crear, modificar y eliminar cuentas de usuario locales.
- Crear, modificar y eliminar cuentas de grupo locales.
- Establecer una política de administración de contraseñas para los usuarios, y bloquear y desbloquear manualmente las cuentas de los usuarios.

Secciones

- Descripción de conceptos de usuarios y grupos (y cuestionario)
- Obtención de acceso de superusuario (y ejercicio guiado)
- Administración de cuentas de usuarios locales (y ejercicio guiado)
- Administración de cuentas de grupos locales (y ejercicio guiado)
- Administración de contraseñas de usuarios (y ejercicio guiado)

Trabajo de laboratorio

Administración de usuarios y grupos locales

Describir conceptos de usuario y grupo

Objetivos

Describir el propósito de los usuarios y grupos en un sistema Linux.

¿Qué es un usuario?

Una cuenta de *usuario* se usa para proporcionar límites de seguridad entre diferentes personas y programas que pueden ejecutar comandos.

Los usuarios tienen *nombres de usuario* para identificarlos como usuarios humanos y facilitar el trabajo. Internamente, el sistema distingue las cuentas de usuario por el número de identificación único que se les asigna, el ID de usuario o *UID*. En la mayoría de los escenarios, si una persona usa una cuenta de usuario, el sistema asigna una *contraseña* secreta para que el usuario demuestre que es el usuario autorizado para iniciar sesión.

Las cuentas de usuario son fundamentales para la seguridad del sistema. Cada proceso (programa en ejecución) en el sistema se ejecuta como un usuario particular. Cada archivo tiene un usuario particular como su propietario. Con la propiedad del archivo, al sistema aplica el control de acceso para los usuarios de los archivos. El usuario que está asociado con un proceso de ejecución determina los archivos y directorios accesibles para ese proceso.

Hay cuentas de usuario de los siguientes tipos principales: el *superusuario*, el *usuario del sistema* y el *usuario normal*.

- La cuenta de *superusuario* administra el sistema. El nombre del superusuario es `root` y la cuenta tiene UID 0. El superusuario tiene acceso completo al sistema.
- El sistema tiene cuentas de *usuario del sistema* que usan los procesos que proporcionan servicios de soporte. Estos procesos, o *daemons* por lo general no necesitan ejecutarse como superusuario. Son cuentas asignadas sin privilegios para proteger sus archivos y otros recursos entre sí y de los usuarios habituales del sistema. Los usuarios no inician sesión de forma interactiva con una cuenta de usuario del sistema.
- La mayoría de los usuarios tienen cuentas de *usuario normal* que usan para su trabajo diario. Al igual que los usuarios del sistema, los usuarios normales tienen acceso limitado al sistema.

Puede usar el comando `id` para mostrar información acerca del usuario con sesión iniciada actualmente:

```
[user01@host ~]$ id
uid=1000(user01) gid=1000(user01) groups=1000(user01)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Para ver información básica sobre otro usuario, envíe el nombre de usuario al comando `id` como argumento:

```
[user01@host ~]$ id user02
uid=1002(user02) gid=1001(user02) groups=1001(user02)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

capítulo 3 | Administración de usuarios y grupos locales

Use el comando `ls -l` para ver el propietario de un archivo. Use el comando `ls -ld` para ver el propietario de un directorio, en lugar del contenido de ese directorio. En la siguiente salida, la tercera columna muestra el nombre de usuario.

```
[user01@host ~]$ ls -l mytextfile.txt
-rw-rw-r-- 1 user01 user01 0 Feb  5 11:10 mytextfile.txt
[user01@host]$ ls -ld Documents
drwxrwxr-x. 2 user01 user01 6 Feb  5 11:10 Documents
```

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 el comando `ps` con la opción `-a` para ver todos los procesos con una terminal. Use el comando `ps` con la opción `-u` para ver el usuario asociado con un proceso. En la siguiente salida, la primera columna muestra el nombre de usuario.

```
[user01@host ~]$ ps -au
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START  TIME COMMAND
root     1690  0.0  0.0 220984  1052  ttyS0   Ss+  22:43  0:00 /sbin/agetty -o -p --
          \u --keep-baud 1
user01   1769  0.0  0.1 377700  6844  tty2    Ssl+ 22:45  0:00 /usr/libexec/gdm-x-
session --register-
user01   1773  1.3  1.3 528948  78356  tty2    Sl+   22:45  0:03 /usr/libexec/Xorg vt2
          -displayfd 3 -au
user01   1800  0.0  0.3 521412  19824  tty2    Ssl+  22:45  0:00 /usr/libexec/gnome-
session-binary
user01   3072  0.0  0.0 224152  5756  pts/1    Ss    22:48  0:00 -bash
user01   3122  0.0  0.0 225556  3652  pts/1    R+   22:49  0:00 ps -au
```

En la salida de los comandos anteriores, se muestran los usuarios por nombre, pero, internamente, el sistema operativo usa UID para realizar un seguimiento de los usuarios. La asignación de nombres de usuario a UID se define en las bases de datos de la información de la cuenta. De forma predeterminada, los sistemas usan el archivo `/etc/passwd` para almacenar información sobre los usuarios locales.

Cada línea del archivo `/etc/passwd` contiene información sobre un usuario. El archivo se divide en siete campos separados por dos puntos. A continuación, se muestra un ejemplo de una línea de `/etc/passwd`:

```
[user01@host ~]$ cat /etc/passwd
...output omitted...
user01:x:1000:1000:User One:/home/user01:/bin/bash
```

Considere cada parte del bloque de código, separada por dos puntos:

- **user01**: Nombre de usuario para este usuario.
- **x**: La contraseña cifrada del usuario se almacenaba históricamente aquí; ahora es un marcador de posición.
- **1000**: El número de UID para esta cuenta de usuario.
- **1000**: El número de GID para el grupo principal de esta cuenta de usuario. Los grupos se analizan más adelante en esta sección.
- **User One**: Un breve comentario, una descripción o el nombre real de este usuario.
- **/home/user01**: El directorio de inicio del usuario y el directorio de trabajo inicial cuando se inicia la shell de inicio de sesión.

- **/bin/bash**: El programa de shell predeterminado para este usuario, que se ejecuta al iniciar sesión. Algunas cuentas usan la shell `/sbin/nologin` para no permitir inicios de sesión interactivos con esa cuenta.

¿Qué es un grupo?

Un grupo es una colección de usuarios que necesitan compartir el acceso a archivos y otros recursos del sistema. Los grupos se pueden usar para otorgar acceso a los archivos a un conjunto de usuarios en lugar de a un solo usuario.

Al igual que los usuarios, los grupos tienen *nombres de grupo* para facilitar el reconocimiento. Internamente, el sistema distingue los grupos por el número de identificación único, el *ID de grupo* o *GID*, que se les asigna. La asignación de nombres de grupo a GID se define en las bases de datos de administración de identidades de la información de la cuenta de grupo. De forma predeterminada, los sistemas usan el archivo `/etc/group` para almacenar información sobre los grupos locales.

Cada línea del archivo `/etc/group` contiene información sobre un grupo. Cada entrada de grupo se divide en cuatro campos separados con dos puntos. A continuación, se muestra un ejemplo de una línea de `/etc/group`:

```
[user01@host ~]$ cat /etc/group
...output omitted...
group01:x:10000:user01,user02,user03
```

Considere cada parte del bloque de código, separada por dos puntos:

- **group01**: Nombre para este grupo.
- **x**: Campo de contraseña de grupo obsoleto; ahora es un marcador de posición.
- **10000**: El número de GID para este grupo (10000).
- **user01, user02, user03**: Una lista de usuarios que son miembros de este grupo como grupo secundario.

Grupos principales y grupos secundarios

Cada usuario tiene exactamente un grupo principal. Para usuarios locales, este es el grupo enumerado por GID en el archivo `/etc/passwd`. El grupo principal es propietario de los archivos que crea el usuario.

Al crear un usuario regular, se crea un grupo con el mismo nombre que el usuario, para que sea el grupo principal para el usuario. El usuario es el único miembro de este *grupo privado de usuarios*. Este diseño de membresía de grupo simplifica la administración de permisos de archivos, para que los grupos de usuarios estén separados de forma predeterminada.

Los usuarios también pueden tener *grupos secundarios*. La pertenencia a grupos secundarios se almacena en el archivo `/etc/group`. A los usuarios se les otorga acceso a los archivos en función de si alguno de sus grupos tiene acceso, más allá de si los grupos son principales o secundarios. Por ejemplo, si el usuario `user01` tiene un grupo principal `user01` y grupos secundarios `wheel` y `webadmin`, entonces ese usuario puede leer archivos legibles para cualquiera de esos tres grupos.

El comando `id` puede mostrar la pertenencia al grupo de un usuario. En el ejemplo anterior, el usuario `user01` tiene el grupo `user01` como su grupo principal (`gid`). El ítem `groups` enumera todas las membresías de grupo para este usuario, y el usuario también tiene los grupos `wheel` y `group01` como grupos secundarios.

```
[user01@host ~]$ id  
uid=1001(user01) gid=1003(user01) groups=1003(user01),10(wheel),10000(webadmin)  
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```



Referencias

Páginas del manual: `id(1)`, `passwd(5)` y `group(5)`

`info libc (GNU C Library Reference Manual)`

- Sección 30: Usuarios y grupos

(El paquete `glibc-devel` se debe haber instalado para que estos nodos de información estén disponibles).

► Cuestionario

Describir conceptos de usuario y grupo

Elija la respuesta correcta para las siguientes preguntas:

- ▶ 1. **¿Qué ítem representa un número que identifica al usuario en el nivel más fundamental?**
 - a. Usuario principal
 - b. UID
 - c. GID
 - d. Username

- ▶ 2. **¿Qué ítem representa el programa que proporciona el prompt de línea de comandos del usuario?**
 - a. Shell principal
 - b. Directorio de inicio
 - c. Shell de inicio de sesión
 - d. Nombre de comando

- ▶ 3. **¿Qué ítem o archivo representa la ubicación de la información del grupo local?**
 - a. Directorio de inicio
 - b. /etc/passwd
 - c. /etc/GID
 - d. /etc/group

- ▶ 4. **¿Qué ítem o archivo representa la ubicación de los archivos personales del usuario?**
 - a. Directorio de inicio
 - b. Shell de inicio de sesión
 - c. /etc/passwd
 - d. /etc/group

- ▶ 5. **¿Qué ítem representa un número que identifica al grupo en el nivel más fundamental?**
 - a. Grupo principal
 - b. UID
 - c. GID
 - d. Groupid

- 6. ¿Qué ítem o archivo representa la ubicación de la información de la cuenta de usuario local?
- a. Directorio de inicio
 - b. /etc/passwd
 - c. /etc/UID
 - d. /etc/group
- 7. ¿Cuál es el cuarto campo del archivo /etc/passwd?
- a. Directorio de inicio
 - b. UID
 - c. Shell de inicio de sesión
 - d. Grupo principal

► Solución

Describir conceptos de usuario y grupo

Elija la respuesta correcta para las siguientes preguntas:

- ▶ 1. **¿Qué ítem representa un número que identifica al usuario en el nivel más fundamental?**
 - a. Usuario principal
 - b. UID
 - c. GID
 - d. Username

- ▶ 2. **¿Qué ítem representa el programa que proporciona el prompt de línea de comandos del usuario?**
 - a. Shell principal
 - b. Directorio de inicio
 - c. Shell de inicio de sesión
 - d. Nombre de comando

- ▶ 3. **¿Qué ítem o archivo representa la ubicación de la información del grupo local?**
 - a. Directorio de inicio
 - b. /etc/passwd
 - c. /etc/GID
 - d. /etc/group

- ▶ 4. **¿Qué ítem o archivo representa la ubicación de los archivos personales del usuario?**
 - a. Directorio de inicio
 - b. Shell de inicio de sesión
 - c. /etc/passwd
 - d. /etc/group

- ▶ 5. **¿Qué ítem representa un número que identifica al grupo en el nivel más fundamental?**
 - a. Grupo principal
 - b. UID
 - c. GID
 - d. Groupid

► 6. ¿Qué ítem o archivo representa la ubicación de la información de la cuenta de usuario local?

- a. Directorio de inicio
- b. /etc/passwd
- c. /etc/UID
- d. /etc/group

► 7. ¿Cuál es el cuarto campo del archivo /etc/passwd?

- a. Directorio de inicio
- b. UID
- c. Shell de inicio de sesión
- d. Grupo principal

Obtención de acceso de superusuario

Objetivos

Cambiar a la cuenta de superusuario para administrar un sistema Linux y otorgar a otros usuarios acceso de superusuario a través del comando `sudo`.

El superusuario

La mayoría de los sistemas operativos tienen un *superusuario*; un usuario que tiene todo el poder sobre el sistema. En Red Hat Enterprise Linux, este es el usuario `root`. Este usuario tiene el poder de anular los privilegios normales del sistema de archivos, y puede usarlo para manejar y administrar el sistema. Para tareas como la instalación o eliminación de software, y para administrar los directorios y los archivos del sistema, los usuarios deben aumentar sus privilegios al usuario `root`.

Por lo general, solo el usuario `root` entre los usuarios normales puede controlar la mayoría de los dispositivos, pero se aplican algunas excepciones. Por ejemplo, los usuarios normales pueden controlar dispositivos desmontables, como dispositivos USB. Por lo tanto, los usuarios normales pueden agregar y eliminar archivos y administrar de otro modo un dispositivo desmontable, pero solo el usuario `root` puede administrar los discos duros 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 de usuario `root` se ve comprometida, el sistema está en peligro y es posible que pierda el control administrativo. Red Hat invita a los administradores a 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 `Administrator` en Microsoft Windows. En Linux, la mayoría de los administradores del sistema inician sesión en el sistema como un usuario sin privilegios y usan distintas herramientas para ganar privilegios de usuario `root` temporalmente.



Advertencia

Los usuarios de Microsoft Windows pueden estar familiarizados con la práctica de iniciar sesión como el usuario local `Administrator` para realizar tareas de administrador del sistema. En la actualidad, no se recomienda esta práctica; los usuarios obtienen privilegios para realizar la administración mediante membresías en el grupo `Administrators`. De manera similar, en RHEL, Red Hat recomienda que los administradores del sistema nunca inicien sesión directamente como `root`. En cambio, los administradores de sistema deben iniciar sesión como usuario normal y usar mecanismos (`su`, `sudo` o `PolicyKit`, por ejemplo) para obtener privilegios de superusuario temporalmente.

Al haber iniciado sesión como `root`, todo el entorno de escritorio se ejecuta sin necesidad con privilegios administrativos. Una vulnerabilidad de seguridad que normalmente podría comprometer solo una cuenta de usuario normal puede poner en peligro todo el sistema.

Cambiar cuentas de usuario

El comando `su` les permite a los usuarios cambiar a una cuenta de usuario diferente. Si ejecuta el comando `su` desde una cuenta de usuario regular con otra cuenta de usuario como parámetro, debe proporcionar la contraseña de la cuenta a la que desea cambiar. Cuando el usuario `root` ejecuta el comando `su`, no es necesario introducir la contraseña del usuario.

Este ejemplo usa el comando `su` de la cuenta `user01` para cambiar a la cuenta `user02`:

```
[user01@host ~]$ su - user02
Password: user02_password
[user02@host ~]$
```

Si omite el nombre de usuario, el comando `su` o `su -` intenta cambiar a `root` de forma predeterminada.

```
[user01@host ~]$ su -
Password: root_password
[root@host ~]#
```

El comando `su` inicia una *shell sin inicio de sesión*, mientras que el comando `su -` (con la opción de guion) inicia una *shell de inicio de sesión*. La diferencia principal entre los dos comandos es que `su -` establece el entorno de la shell como si iniciara una sesión nueva como ese usuario, mientras que `su` inicia una shell como ese usuario, pero usa la configuración de entorno del usuario original.

En la mayoría de los casos, los administradores deben ejecutar `su -` para obtener una shell con la configuración de entorno normal del usuario de destino. Si desea obtener más información, consulte la página del manual `bash(1)`.



nota

El uso más frecuente del comando `su` es obtener una interfaz de línea de comandos (prompt de shell) que se ejecuta como otro usuario, generalmente `root`. Sin embargo, se puede usar el comando `su` con la opción `-c` para ejecutar un programa arbitrario como otro usuario. Este comportamiento es similar a la utilidad de Windows `runas`. Ejecute `info su` para ver más detalles.

Ejecución de comandos con Sudo

Por razones de seguridad, en algunos casos, los administradores del sistema configuran el usuario `root` para que no tenga una contraseña válida. Por lo tanto, los usuarios no pueden iniciar sesión en el sistema como `root` directamente con una contraseña. Además, no puede usar `su` para obtener una shell interactiva. En este caso, puede usar el comando `sudo` para obtener acceso a `root`.

A diferencia del comando `su`, `sudo` por lo general requiere que un usuario ingrese su propia contraseña para la autenticación y no la contraseña de la cuenta a la que intenta acceder. Es decir, los usuarios que usan `sudo` para ejecutar comandos como `root` no necesitan saber la contraseña `root`. En su lugar, usan sus propias contraseñas para autenticar el acceso.

En la siguiente tabla, se resumen las diferencias entre los comandos `su`, `su -` y `sudo`:

	su	su -	sudo
Conviértase en nuevo usuario	Sí	Sí	Por comando escalado
Entorno	Usuario actual	Nuevo usuario	Usuario actual
Se requiere contraseña	Nuevo usuario	Nuevo usuario	Usuario actual
Privilegios	Igual que el nuevo usuario	Igual que el nuevo usuario	Definido por configuración
Actividad registrada	Solo comando su	Solo comando su	Por comando escalado

Además, puede configurar el comando **sudo** para permitir que usuarios específicos ejecuten cualquier comando como otro usuario, o solo algunos comandos como ese usuario. Por ejemplo, cuando **sudo** se configura para permitir al usuario **user01** ejecutar el comando **usermod** como **root**, puede ejecutar el siguiente comando a fin de bloquear o desbloquear una cuenta de usuario:

```
[user01@host ~]$ sudo usermod -L user02
[sudo] password for user01: user01_password
[user01@host ~]$ su - user02
Password: user02_password
su: Authentication failure
[user01@host ~]$
```

Si un usuario intenta ejecutar un comando como otro usuario, y la configuración de **sudo** no lo permite, el bash bloquea el comando, se registra el intento y, de forma predeterminada, se enviará un correo electrónico al usuario **root**.

```
[user02@host ~]$ sudo tail /var/log/secure
[sudo] password for user02: user02_password
user02 is not in the sudoers file. This incident will be reported.
[user02@host ~]$
```

Otro beneficio de **sudo** es registrar de manera predeterminada todos los comandos ejecutados en **/var/log/secure**.

```
[user01@host ~]$ sudo tail /var/log/secure
...output omitted...
Mar  9 20:45:46 host sudo[2577]: user01 : TTY=pts/0 ; PWD=/home/user01 ;
USER=root ; COMMAND=/sbin/usermod -L user02
...output omitted...
```

En Red Hat Enterprise Linux 7 y versiones posteriores, todos los miembros del grupo **wheel** pueden usar **sudo** para ejecutar comandos como cualquier usuario, incluido el usuario **root**, usando su propia contraseña.

**Advertencia**

Históricamente, los sistemas UNIX usan la membresía en el grupo `wheel` para otorgar o controlar el acceso como superusuario. RHEL 6 no otorgó ningún privilegio especial al grupo `wheel` de manera predeterminada. Los administradores de sistemas que hayan usado anteriormente este grupo para un propósito no estándar deben actualizar una configuración anterior, para evitar que usuarios inesperados y no autorizados obtengan acceso administrativo en RHEL 7 y sistemas posteriores.

Obtención de una shell de root interactiva con Sudo

Para acceder a la cuenta `root` con `sudo`, use el comando `sudo -i`. Este comando cambia a la cuenta `root` y ejecuta la shell predeterminada de ese usuario (generalmente `bash`) y los scripts de inicio de sesión interactivos asociados. Para ejecutar la shell sin los scripts interactivos, use el comando `sudo -s`.

Por ejemplo, un administrador puede obtener una shell interactiva como `root` en una instancia de AWS Elastic Cloud Computing (EC2) al usar una autenticación de clave pública de SSH para iniciar sesión como el usuario normal `ec2-user` y, luego, ejecutar `sudo -i` para obtener la shell del usuario `root`.

```
[ec2-user@host ~]$ sudo -i
[sudo] password for ec2-user: ec2-user_password
[root@host ~]#
```

Configuración de Sudo

El archivo `/etc/sudoers` es el archivo de configuración principal del comando `sudo`. Para evitar problemas si varios administradores intentan editar el archivo al mismo tiempo, puede editarlo solo con el comando especial `visudo`. El editor `visudo` también valida el archivo para garantizar que no haya errores de sintaxis.

Por ejemplo, la siguiente línea del archivo `/etc/sudoers` habilita el acceso `sudo` para miembros del grupo `wheel`:

```
%wheel      ALL=(ALL:ALL)      ALL
```

- La cadena `%wheel` es el usuario o grupo al que se aplica la regla. El símbolo `%` antes de la palabra `wheel` especifica un grupo.
- El comando `ALL=(ALL:ALL)` especifica que en cualquier host con este archivo (el primer `ALL`), los usuarios en el grupo `wheel` pueden ejecutar comandos como cualquier otro usuario (el segundo `ALL`) y cualquier otro grupo (el tercero `ALL`) en el sistema.
- El comando final `ALL` especifica que los usuarios en el grupo `wheel` pueden ejecutar cualquier comando.

De forma predeterminada, el archivo `/etc/sudoers` también incluye el contenido de cualquier archivo del directorio `/etc/sudoers.d` como parte del archivo de configuración. Con esta jerarquía, puede agregar el acceso `sudo` para un usuario simplemente al colocar un archivo apropiado en ese directorio.

**nota**

Es conveniente colocar los archivos de configuración en el directorio `/etc/sudoers.d`. Puede habilitar o deshabilitar el acceso sudo al copiar un archivo en el directorio o eliminándolo de él.

En este curso, creará y eliminará archivos en el directorio `/etc/sudoers.d` para configurar el acceso sudo para usuarios y grupos.

Para habilitar el acceso sudo completo para el usuario `user01`, puede crear el archivo `/etc/sudoers.d/user01` con el siguiente contenido:

```
user01    ALL=(ALL)    ALL
```

Para habilitar el acceso sudo completo para el grupo `group01`, puede crear el archivo `/etc/sudoers.d/group01` con el siguiente contenido:

```
%group01    ALL=(ALL)    ALL
```

Para permitir que los usuarios en el grupo `games` ejecuten el comando `id` como el usuario `operator`, puede crear el archivo `/etc/sudoers.d/games` con el siguiente contenido:

```
%games    ALL=(operator)    /bin/id
```

También es posible configurar sudo para permitir que un usuario ejecute comandos como otro usuario sin ingresar su contraseña, con el comando `NOPASSWD: ALL`:

```
ansible    ALL=(ALL)    NOPASSWD: ALL
```

Si bien otorgar este nivel de acceso a un usuario o grupo implica riesgos de seguridad evidentes, los administradores del sistema usan este enfoque con frecuencia en instancias de la nube, máquinas virtuales y sistemas de aprovisionamiento para facilitar la configuración de servidores. La cuenta con este acceso se debe proteger cuidadosamente y puede requerir autenticación de clave pública de SSH para que un usuario que se encuentra en un sistema remoto pueda acceder a ella.

Por ejemplo, Amazon Machine Image (AMI) oficial de Red Hat Enterprise Linux en Amazon Web Services Marketplace se envía con las contraseñas `root` y `ec2-user` bloqueadas. La cuenta `ec2-user` está configurada para permitir el acceso interactivo remoto a través de la autenticación de clave pública de SSH. El usuario `ec2-user` también puede ejecutar cualquier comando como `root` sin contraseña debido a que la última línea del archivo `/etc/sudoers` de AMI está configurada de la siguiente manera:

```
ec2-user    ALL=(ALL)    NOPASSWD: ALL
```

El requisito de ingresar una contraseña para sudo puede volverse a habilitar o pueden hacerse otros cambios para reforzar la seguridad como parte de la configuración del sistema.



Referencias

Páginas del manual: su(1), sudo(8), visudo(8) y sudoers(5)

`info libc persona (GNU C Library Reference Manual)`

- Sección 30.2: "The Persona of a Process"

(El paquete `glibc-doc` se debe haber instalado para que estos nodos de información estén disponibles).

► Ejercicio Guiado

Obtención de acceso de superusuario

En este ejercicio, practica cambiar a la cuenta `root` y ejecutar comandos como `root`.

Resultados

- Usar el comando `sudo` para cambiar al usuario `root` y acceder a la shell interactiva como `root` sin tener que saber la contraseña del superusuario.
- Explicar cómo los comandos `su` y `sudo` - pueden afectar al entorno de la shell al ejecutar o no ejecutar los scripts de inicio de sesión.
- Usar el comando `sudo` para ejecutar otros comandos como el usuario `root`.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start users-superuser
```

Instrucciones

- 1. En `workstation`, abra una sesión de SSH servera como el usuario `student`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

- 2. Explore el entorno de la shell del usuario `student`. Visualice la información del usuario y del grupo actual, y muestre el directorio de trabajo actual. También vea las variables de entorno que especifican el directorio de inicio del usuario y las ubicaciones de los archivos ejecutables del usuario.

2.1. Ejecute `id` para ver la información del usuario y grupo actual.

```
[student@servera ~]$ id
uid=1000(student) gid=1000(student) groups=1000(student),10(wheel)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

2.2. Ejecute `pwd` para ver el directorio de trabajo actual.

```
[student@servera ~]$ pwd
/home/student
```

- 2.3. Imprima los valores de las variables HOME y PATH para determinar el directorio de inicio y la ruta de los archivos ejecutables del usuario, respectivamente.

```
[student@servera ~]$ echo $HOME  
/home/student  
[student@servera ~]$ echo $PATH  
/home/student/.local/bin:/home/student/bin:/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin
```

- 3. Cambie al usuario root en una shell sin inicio de sesión y explore el nuevo entorno de la shell.

- 3.1. Ejecute el comando sudo su en el prompt de shell para convertirse en el usuario root.

```
[student@servera ~]$ sudo su  
[sudo] password for student: student  
[root@servera student]#
```

- 3.2. Ejecute id para ver la información del usuario y grupo actual.

```
[root@servera student]# id  
uid=0(root) gid=0(root) groups=0(root)  
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

- 3.3. Ejecute pwd para ver el directorio de trabajo actual.

```
[root@servera student]# pwd  
/home/student
```

- 3.4. Imprima los valores de las variables HOME y PATH para determinar el directorio de inicio y la ruta de los archivos ejecutables del usuario, respectivamente.

```
[root@servera student]# echo $HOME  
/root  
[root@servera student]# echo $PATH  
/root/.local/bin:/root/bin:/sbin:/bin:/usr/sbin:/usr/bin:/usr/local/sbin:/usr/local/bin
```

Cuando usa el comando su para convertirse en el usuario root, no conserva la ruta actual del usuario student. Como puede ver en el siguiente paso, la ruta tampoco es la ruta del usuario root.

¿Qué sucedió? La diferencia es que no ejecuta su directamente. En cambio, ejecutó el comando su como el usuario root mediante sudo porque no cuenta con la contraseña del superusuario. El comando sudo inicialmente anula la variable PATH del entorno por razones de seguridad. Cualquier comando que se ejecute después de la anulación inicial todavía puede actualizar la variable PATH, como puede ver en los siguientes pasos.

- 3.5. Salga de la shell del usuario root para volver a la shell del usuario student.

```
[root@servera student]# exit
exit
[student@servera ~]$
```

- 4. Cambie al usuario `root` en una shell con inicio de sesión y explore el nuevo entorno de la shell.

- 4.1. Ejecute el comando `sudo su -` en el prompt de shell para convertirse en el usuario `root`.

El comando `sudo` puede o no pedirle la contraseña de `student`, según el período de espera de `sudo`. El período de espera predeterminado es de cinco minutos. Si se ha autenticado en `sudo` en los últimos cinco minutos, el comando `sudo` no le pedirá la contraseña. Si han transcurrido más de cinco minutos desde que se autenticó en `sudo`, debe ingresar `student` como la contraseña para la autenticación en `sudo`.

```
[student@servera ~]$ sudo su -
[root@servera ~]#
```

Observe la diferencia en el prompt de shell en comparación con el de `sudo su` en el paso anterior.

- 4.2. Ejecute `id` para ver la información del usuario y grupo actual.

```
[root@servera ~]# id
uid=0(root) gid=0(root) groups=0(root)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

- 4.3. Ejecute `pwd` para ver el directorio de trabajo actual.

```
[root@servera ~]# pwd
/root
```

- 4.4. Imprima los valores de las variables `HOME` y `PATH` para determinar el directorio de inicio y la ruta de los archivos ejecutables del usuario, respectivamente.

```
[root@servera ~]# echo $HOME
/root
[root@servera ~]# echo $PATH
/root/.local/bin:/root/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin
```

Como en el paso anterior, después de que el comando `sudo` restableció la variable `PATH` en la configuración del entorno de shell del usuario `student`, el comando `su -` ejecutó los scripts de inicio de sesión de la shell para `root` y estableció la variable `PATH` con otro valor. El comando `su` sin la opción de guion (-) no tiene el mismo comportamiento.

- 4.5. Salga de la shell del usuario `root` para volver a la shell del usuario `student`.

```
[root@servera ~]# exit
logout
[student@servera ~]$
```

- 5. Verifique que el usuario **operator1** pueda ejecutar cualquier comando como cualquier usuario mediante el uso del comando **sudo**.

```
[student@servera ~]$ sudo cat /etc/sudoers.d/operator1  
operator1 ALL=(ALL) ALL
```

- 6. Conviértase en el usuario **operator1** y vea el contenido del archivo **/var/log/messages**. Copie el archivo **/etc/motd** en **/etc/motdOLD**. Quite el archivo **/etc/motdOLD**. Dado que estas operaciones requieren derechos administrativos, use el comando **sudo** para ejecutar esos comandos como el superusuario. No cambie a root usando **sudo su** o **sudo su -**. Use **redhat** como la contraseña del usuario **operator1**.

- 6.1. Cambie al usuario **operator1**.

```
[student@servera ~]$ su - operator1  
Password: redhat  
[operator1@servera ~]$
```

- 6.2. Intente ver las últimas cinco líneas de **/var/log/messages** sin usar **sudo**. No debería poder.

```
[operator1@servera ~]$ tail -5 /var/log/messages  
tail: cannot open '/var/log/messages' for reading: Permission denied
```

- 6.3. Intente ver las últimas cinco líneas de **/var/log/messages** usando **sudo**. Debe ser capaz de realizarse de manera correcta. Ejemplo de resultado: Regrese al sistema **workstation** como el usuario **student**.

```
[operator1@servera ~]$ sudo tail -5 /var/log/messages  
[sudo] password for operator1: redhat  
Mar 9 15:53:36 servera su[2304]: FAILED SU (to operator1) student on pts/1  
Mar 9 15:53:51 servera su[2307]: FAILED SU (to operator1) student on pts/1  
Mar 9 15:53:58 servera su[2310]: FAILED SU (to operator1) student on pts/1  
Mar 9 15:54:12 servera su[2322]: (to operator1) student on pts/1  
Mar 9 15:54:25 servera su[2353]: (to operator1) student on pts/1
```



nota

La salida anterior puede diferir en su sistema.

- 6.4. Intente copiar **/etc/motd** como **/etc/motdOLD** sin usar **sudo**. No debería poder.

```
[operator1@servera ~]$ cp /etc/motd /etc/motdOLD  
cp: cannot create regular file '/etc/motdOLD': Permission denied
```

- 6.5. Intente hacer una copia de **/etc/motd** como **/etc/motdOLD** usando **sudo**. Debe ser capaz de realizarse de manera correcta.

```
[operator1@servera ~]$ sudo cp /etc/motd /etc/motdOLD  
[operator1@servera ~]$
```

6.6. Intente eliminar /etc/motdOLD sin usar sudo. No debería poder.

```
[operator1@servera ~]$ rm /etc/motdOLD  
rm: remove write-protected regular empty file '/etc/motdOLD'? y  
rm: cannot remove '/etc/motdOLD': Permission denied  
[operator1@servera ~]$
```

6.7. Intente eliminar /etc/motdOLD usando sudo. Debe ser capaz de realizarse de manera correcta.

```
[operator1@servera ~]$ sudo rm /etc/motdOLD  
[operator1@servera ~]$
```

6.8. Regrese al sistema workstation como el usuario student.

```
[operator1@servera ~]$ exit  
logout  
[student@servera ~]$ exit  
logout  
Connection to servera closed.  
[student@workstation ~]$
```

Finalizar

En la máquina **workstation**, cambie al directorio de inicio de usuario **student** y use el comando **lab** para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish users-superuser
```

Esto concluye la sección.

Administración de cuentas de usuarios locales

Objetivos

Crear, modificar y eliminar cuentas de usuario locales.

Administración de usuarios locales

Se pueden usar distintas herramientas de la línea de comandos para administrar cuentas de usuarios locales. En esta sección se revisan algunas de las más importantes.

Creación de usuarios desde la línea de comandos

El comando `useradd username` crea un usuario llamado `username`. Configura el directorio de inicio del usuario y la información de la cuenta, y crea un grupo privado para el usuario denominado `username`. En este punto, la cuenta no tiene configurada una contraseña válida y el usuario no puede iniciar sesión hasta que se defina una.

El comando `useradd --help` muestra las opciones básicas para anular los valores predeterminados. En la mayoría de los casos, puede usar las mismas opciones 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 establecen desde el archivo `/etc/login.defs`. Los valores de este archivo afectan solo a las cuentas de usuario creadas recientemente. Un cambio en este archivo no afectará a los usuarios existentes.

En Red Hat Enterprise Linux9, el comando `useradd` asigna a los nuevos usuarios el primer UID libre mayor o igual a 1000, a menos que especifique explícitamente uno mediante la opción `-u`.

Modificación de usuarios existentes desde la línea de comandos

El comando `usermod --help` muestra las opciones básicas para modificar una cuenta. Algunas opciones comunes son las siguientes:

Opciones de usermod:	Uso
<code>-a, --append</code>	Se usa con la opción <code>-G</code> para agregar los grupos secundarios al conjunto actual de membresías de grupo del usuario en lugar de reemplazar el conjunto de grupos secundarios con un nuevo conjunto.
<code>-c, --comment COMMENT</code>	Agregar el texto <code>COMMENT</code> en el campo de comentarios.
<code>-d, --home HOME_DIR</code>	Especificar un directorio de inicio para la cuenta de usuario.

Opciones de usermod:	Uso
-g, --gid GROUP	Especificar el grupo principal para la cuenta de usuario.
-G, --groups GROUPS	Especificar una lista de grupos secundarios separados por comas para la cuenta de usuario.
-L, --lock	Bloquear la cuenta de usuario.
-m, --move-home	Mover el directorio de inicio del usuario a una nueva ubicación. Debe usarlo con la opción -d.
-s, --shell SHELL	Especificar una shell de inicio de sesión particular para la cuenta de usuario.
-U, --unlock	Desbloquear la cuenta de usuario.

Eliminación de usuarios desde la línea de comandos

El comando `userdel username` elimina al usuario `username` de `/etc/passwd`, pero deja el directorio de inicio del usuario intacto. El comando `userdel -r username` elimina al usuario de `/etc/passwd`, así como el directorio de inicio del usuario.



Advertencia

Cuando elimina un usuario sin especificar la opción `userdel -r`, los archivos del usuario ahora son propiedad de un UID no asignado. Si crea un usuario y a ese usuario se le asigna el UID del usuario eliminado, la nueva cuenta será propietaria de esos archivos, lo que supone un riesgo para la seguridad. Por lo general, las políticas de seguridad de la organización no permiten la eliminación de cuentas de usuario y, en cambio, bloquean su uso para evitar este escenario.

En el siguiente ejemplo, se demuestra cómo esto puede conducir a una fuga de información:

```
[root@host ~]# useradd user01
[root@host ~]# ls -l /home
drwx----- 3 user01 user01 74 Mar 4 15:22 user01
[root@host ~]# userdel user01
[root@host ~]# ls -l /home
drwx----- 3 1000 1000 74 Mar 4 15:22 user01
[root@host ~]# useradd -u 1000 user02
[root@host ~]# ls -l /home
drwx----- 3 user02 user02 74 Mar 4 15:23 user02
drwx----- 3 user02 user02 74 Mar 4 15:22 user01
```

Observe que `user02` ahora es propietario de todos los archivos que pertenecieron a `user01`. El usuario `root` puede usar el comando `find / -nouser -o -nogroup` para encontrar todos los archivos y directorios que no pertenecen a nadie.

Configuración de contraseñas desde la línea de comandos

El comando `passwd username` define la contraseña inicial o cambia la contraseña existente del usuario `username`. El usuario `root` puede definir una contraseña en cualquier valor. El terminal muestra un mensaje si la contraseña no cumple con los criterios mínimos recomendados, pero puede volver a ingresar la contraseña nueva y el comando `passwd` la actualiza correctamente.

```
[root@host ~]# passwd user01
Changing password for user user01.
New password: redhat
BAD PASSWORD: The password is shorter than 8 characters
Retype new password: redhat
passwd: all authentication tokens updated successfully.
[root@host ~]#
```

Un usuario regular debe elegir una contraseña de al menos ocho caracteres. No use una palabra del diccionario, el nombre de usuario ni la contraseña anterior.

Rangos de UID

Red Hat Enterprise Linux usa números y rangos de números de UID específicos con fines específicos.

- **UID 0:** el UID de la cuenta de superusuario (`root`).
- **UID 1-200:** UID de la cuenta del sistema asignados estáticamente a los procesos del sistema.
- **UID 201-999:** UID asignados a procesos del sistema que no poseen archivos en este sistema. El software que requiere un UID sin privilegios se asigna dinámicamente desde este conjunto (pool) disponible.
- **UID 1000+:** el rango de UID para asignar a usuarios regulares sin privilegios.



nota

RHEL 6 y las versiones anteriores usan UID en el rango de 1 a 499 para usuarios del sistema y UID superiores a 500 para usuarios regulares. Puede cambiar los rangos predeterminados `useradd` y `groupadd` en el archivo `/etc/login.defs`.



Referencias

Páginas del manual: `useradd(8)`, `usermod(8)` y `userdel(8)`

► Ejercicio Guiado

Administración de cuentas de usuarios locales

En este ejercicio, crea varios usuarios en su sistema y establece contraseñas para esos usuarios.

Resultados

- Configurar un sistema Linux con cuentas de usuario adicionales.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start users-user
```

Instrucciones

- 1. Desde `workstation`, abra una sesión de SSH en `servera` como el usuario `student` y cambie al usuario `root`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

- 2. Cree el usuario `operator1` y confirme que existe en el sistema.

```
[root@servera ~]# useradd operator1
[root@servera ~]# tail /etc/passwd
...output omitted...
operator1:x:1002:1002::/home/operator1:/bin/bash
```

- 3. Establezca la contraseña de `operator1` en `redhat`.

```
[root@servera ~]# passwd operator1
Changing password for user operator1.
New password: redhat
BAD PASSWORD: The password is shorter than 8 characters
Retype new password: redhat
passwd: all authentication tokens updated successfully.
```

- 4. Cree los usuarios adicionales **operator2** y **operator3**. Establezca sus contraseñas como **redhat**.

- 4.1. Agregue el usuario **operator2**. Establezca la contraseña de **operator2** en **redhat**.

```
[root@servera ~]# useradd operator2
[root@servera ~]# passwd operator2
Changing password for user operator2.
New password: redhat
BAD PASSWORD: The password is shorter than 8 characters
Retype new password: redhat
passwd: all authentication tokens updated successfully.
```

- 4.2. Agregue el usuario **operator3**. Establezca la contraseña de **operator3** en **redhat**.

```
[root@servera ~]# useradd operator3
[root@servera ~]# passwd operator3
Changing password for user operator3.
New password: redhat
BAD PASSWORD: The password is shorter than 8 characters
Retype new password: redhat
passwd: all authentication tokens updated successfully.
```

- 5. Actualice las cuentas de usuario **operator1** y **operator2** para incluir los comentarios **Operator One** y **Operator Two**, respectivamente. Verifique que existan los comentarios para las cuentas de usuario.

- 5.1. Ejecute el comando **usermod -c** para actualizar los comentarios de la cuenta de usuario **operator1**.

```
[root@servera ~]# usermod -c "Operator One" operator1
```

- 5.2. Ejecute el comando **usermod -c** para actualizar los comentarios de la cuenta de usuario **operator2**.

```
[root@servera ~]# usermod -c "Operator Two" operator2
```

- 5.3. Vea el archivo **/etc/passwd** para confirmar que existen los comentarios para cada uno de los usuarios **operator1** y **operator2**.

```
[root@servera ~]# tail /etc/passwd
...output omitted...
operator1:x:1002:1002:Operator One:/home/operator1:/bin/bash
operator2:x:1003:1003:Operator Two:/home/operator2:/bin/bash
operator3:x:1004:1004::/home/operator3:/bin/bash
```

- 6. Elimine el usuario **operator3** junto con cualquier dato personal del usuario. Confirme que **operator3** no existe.

- 6.1. Elimine el usuario **operator3** del sistema.

```
[root@servera ~]# userdel -r operator3
```

6.2. Confirme que el usuario operator3 no existe.

```
[root@servera ~]# tail /etc/passwd  
...output omitted...  
operator1:x:1002:1002:Operator One:/home/operator1:/bin/bash  
operator2:x:1003:1003:Operator Two:/home/operator2:/bin/bash
```

Tenga en cuenta que la salida anterior no muestra la información de la cuenta de usuario de operator3.

6.3. Confirme que la carpeta de inicio del usuario operator3 no existe.

```
[root@servera ~]# ls -l /home  
total 0  
drwx----- 4 devops devops 90 Mar 3 09:59 devops  
drwx----- 2 operator1 operator1 62 Mar 9 10:19 operator1  
drwx----- 2 operator2 operator2 62 Mar 9 10:19 operator2  
drwx----- 3 student student 95 Mar 3 09:49 student
```

6.4. Salga de la shell del usuario root para volver a la shell del usuario student.

```
[root@servera ~]# exit  
logout  
[student@servera ~]$
```

6.5. Cierre sesión en servera.

```
[student@servera ~]$ exit  
logout  
Connection to servera closed.  
[student@workstation ~]$
```

Finalizar

En la máquina workstation, cambie al directorio de inicio de usuario student y use el comando lab para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish users-user
```

Esto concluye la sección.

Administración de cuentas de grupos locales

Objetivos

Crear, modificar y eliminar cuentas de grupo locales.

Administración de grupos locales

Varias herramientas de línea de comandos facilitan la administración de grupos. Si bien puede usar la utilidad **Users GUI** para administrar grupos, Red Hat recomienda usar herramientas de línea de comandos.

Creación de grupos desde la línea de comandos

El comando **groupadd** crea grupos. Sin opciones, el comando **groupadd** emplea la siguiente GID disponible de un rango especificado por las variables **GID_MIN** y **GID_MAX** en el archivo **/etc/login.defs**. De manera predeterminada, el comando asigna un valor de GID mayor que cualquier otro GID existente, incluso si hay un valor menor disponible.

El comando **groupadd** con la opción **-g** especifica un GID particular para que el grupo use.

```
[root@host ~]# groupadd -g 10000 group01
[root@host ~]# tail /etc/group
...output omitted...
group01:x:10000:
```



nota

Debido a la creación automática de grupos privados de usuarios (GID 1000+), algunos administradores reservan un rango separado de GID para crear grupos secundarios con otros fines. Sin embargo, esta administración adicional no es necesaria, ya que el UID y el GID primario de un usuario no necesitan ser el mismo número.

El comando **groupadd** con la opción **-r** crea grupos del sistema. Al igual que con los grupos normales, los grupos del sistema usan un GID del rango de GID del sistema válidos enumerados en el archivo **/etc/login.defs**. Los ítems de configuración **SYS_GID_MIN** y **SYS_GID_MAX** en el archivo **/etc/login.defs** definen el rango de GID del sistema.

```
[root@host ~]# groupadd -r group02
[root@host ~]# tail /etc/group
...output omitted...
group01:x:10000:
group02:x:988:
```

Modificación de grupos existentes desde la línea de comandos

El comando `groupmod` cambia las propiedades de un grupo existente. El comando `groupmod` con la opción `-n` especifica un nuevo nombre para el grupo.

```
[root@host ~]# groupmod -n group0022 group02
[root@host ~]# tail /etc/group
...output omitted...
group0022:x:988:
```

Observe que el nombre del grupo se actualiza a `group0022` desde `group02`. El comando `groupmod` con la opción `-g` especifica un nuevo GID.

```
[root@host ~]# groupmod -g 20000 group0022
[root@host ~]# tail /etc/group
...output omitted...
group0022:x:20000:
```

Tenga en cuenta que el GID se modifica a `20000` desde `988`.

Eliminación de grupos desde la línea de comandos

El comando `groupdel` elimina grupos.

```
[root@host ~]# groupdel group0022
```



nota

No puede eliminar un grupo si es el grupo principal de un usuario existente. De manera similar a usar el comando `userdel`, verifique primero para asegurarse de ubicar los archivos que son propiedad del grupo.

Cambio de membresía de grupo desde la línea de comandos

La membresía de un grupo se controla con la administración de usuarios. Use el comando `usermod -g` para cambiar el grupo principal de un usuario.

```
[root@host ~]# id user02
uid=1006(user02) gid=1008(user02) groups=1008(user02)
[root@host ~]# usermod -g group01 user02
[root@host ~]# id user02
uid=1006(user02) gid=10000(group01) groups=10000(group01)
```

Use el comando `usermod -aG` para agregar un usuario a un grupo secundario.

```
[root@host ~]# id user03
uid=1007(user03) gid=1009(user03) groups=1009(user03)
[root@host ~]# usermod -aG group01 user03
[root@host ~]# id user03
uid=1007(user03) gid=1009(user03) groups=1009(user03),10000(group01)
```

**Importante**

El comando `usermod` con la opción `-a` habilita el modo de *adición*. Sin la opción `-a`, el comando elimina al usuario de cualquiera de sus grupos secundarios actuales que no estén incluidos en la lista de la opción `-G`.

Compare la membresía del grupo primario y secundario

El grupo principal de un usuario es el grupo que se ve en la cuenta del usuario en el archivo `/etc/passwd`. Un usuario solo puede pertenecer a un grupo primario a la vez.

Los grupos secundarios de un usuario son los grupos adicionales configurados para el usuario y visualizados en la entrada del usuario en el archivo `/etc/group`. Un usuario puede pertenecer a tantos grupos secundarios como sea necesario para implementar el acceso a los archivos y los permisos de manera efectiva.

Con el fin de configurar permisos de archivos basados en grupos, no hay diferencia entre los grupos primarios y secundarios de un usuario. Si el usuario pertenece a un grupo al que se le ha asignado acceso a archivos específicos, ese usuario tiene acceso a esos archivos.

La única distinción entre las membresías principales y secundarias de un usuario es cuando un usuario crea un archivo. Los archivos nuevos deben tener un propietario de usuario y un propietario de grupo, que se asigna a medida que se crea el archivo. El grupo primario del usuario se usa para la propiedad del grupo del nuevo archivo, a menos que se anule con las opciones del comando.

Cambiar temporalmente su grupo principal

Solo se usa el grupo primario de un usuario para los atributos de creación de archivos nuevos. Sin embargo, puede cambiar temporalmente su grupo primario a otro grupo, pero solo puede elegir entre los grupos secundarios a los que ya pertenece. Puede cambiar si está a punto de crear varios archivos nuevos, manualmente o con scripts, y desea que tengan un grupo diferente asignado como propietario a medida que se crean.

Use el comando `newgrp` para cambiar su grupo primario, en esta sesión de shell. Puede cambiar entre cualquier grupo primario o secundario al que pertenezca, pero solo uno a la vez puede ser primario. Su grupo primario volverá al valor predeterminado si cierra la sesión y vuelve a iniciarla. En este ejemplo, el grupo denominado `group01` se convierte temporalmente en el grupo principal de este usuario.

```
[user03@host ~]# id
uid=1007(user03) gid=1009(user03) groups=1009(user03),10000(group01)
[user03@host ~]$ newgrp group01
[user03@host ~]# id
uid=1007(user03) gid=10000(group01) groups=1009(user03),10000(group01)
```

**Referencias**

Páginas del manual: `group(5)`, `groupadd(8)`, `groupdel(8)` y `usermod(8)`

► Ejercicio Guiado

Administración de cuentas de grupos locales

En este ejercicio, creará grupos, los usará como grupos secundarios para algunos usuarios sin cambiar los grupos principales de esos usuarios y configurará uno de los grupos con acceso sudo para ejecutar comandos como root.

Resultados

- Crear grupos y usarlos como grupos secundarios.
- Configurar acceso sudo para un grupo.

Antes De Comenzar

Con el usuario student en la máquina workstation, use el comando lab para preparar el sistema para este ejercicio.

Este comando crea las cuentas de usuario necesarias para configurar el entorno correctamente.

```
[student@workstation ~]$ lab start users-group
```

Instrucciones

- 1. Desde workstation, abra una sesión de SSH en servera como el usuario student y cambie al usuario root.

```
[student@workstation ~]$ ssh student@servera  
...output omitted...  
[student@servera ~]$ sudo -i  
[sudo] password for student: student  
[root@servera ~]#
```

- 2. Cree el grupo secundario operators con el GID de 30000.

```
[root@servera ~]# groupadd -g 30000 operators
```

- 3. Cree el grupo secundario admin sin especificar un GID.

```
[root@servera ~]# groupadd admin
```

- 4. Verifique que el grupo secundario operators y el grupo secundario admin existan.

```
[root@servera ~]# tail /etc/group
...output omitted...
operators:x:30000:
admin:x:30001:
```

- 5. Asegúrese de que los usuarios operator1, operator2 y operator3 pertenecen al grupo operators.

5.1. Agregue los usuarios operator1, operator2 y operator3 al grupo operators.

```
[root@servera ~]# usermod -aG operators operator1
[root@servera ~]# usermod -aG operators operator2
[root@servera ~]# usermod -aG operators operator3
```

5.2. Confirme que los usuarios estén en el grupo.

```
[root@servera ~]# id operator1
uid=1002(operator1) gid=1002(operator1) groups=1002(operator1),30000(operators)
[root@servera ~]# id operator2
uid=1003(operator2) gid=1003(operator2) groups=1003(operator2),30000(operators)
[root@servera ~]# id operator3
uid=1004(operator3) gid=1004(operator3) groups=1004(operator3),30000(operators)
```

- 6. Asegúrese de que los usuarios sysadmin1, sysadmin2 y sysadmin3 pertenecen al grupo admin. Habilite los derechos administrativos para todos los miembros del grupo admin. Verifique que cualquier miembro del grupo admin pueda ejecutar comandos administrativos.

6.1. Agregue los usuarios sysadmin1, sysadmin2 y sysadmin3 al grupo admin.

```
[root@servera ~]# usermod -aG admin sysadmin1
[root@servera ~]# usermod -aG admin sysadmin2
[root@servera ~]# usermod -aG admin sysadmin3
```

6.2. Confirme que los usuarios estén en el grupo.

```
[root@servera ~]# id sysadmin1
uid=1005(sysadmin1) gid=1005(sysadmin1) groups=1005(sysadmin1),30001(admin)
[root@servera ~]# id sysadmin2
uid=1006(sysadmin2) gid=1006(sysadmin2) groups=1006(sysadmin2),30001(admin)
[root@servera ~]# id sysadmin3
uid=1007(sysadmin3) gid=1007(sysadmin3) groups=1007(sysadmin3),30001(admin)
```

6.3. Examine el archivo /etc/group para comprobar las membresías de grupos secundarios.

```
[root@servera ~]# tail /etc/group
...output omitted...
operators:x:30000:operator1,operator2,operator3
admin:x:30001:sysadmin1,sysadmin2,sysadmin3
```

- 6.4. Cree el archivo `/etc/sudoers.d/admin` para que los miembros del grupo `admin` tengan privilegios administrativos completos.

```
[root@servera ~]# echo "%admin ALL=(ALL) ALL" >> /etc/sudoers.d/admin
```

- 6.5. Cambie al usuario `sysadmin1` (un miembro del grupo `admin`) y asegúrese de poder ejecutar un comando `sudo`.

```
[root@servera ~]# su - sysadmin1
[sysadmin1@servera ~]$ sudo cat /etc/sudoers.d/admin
[sudo] password for sysadmin1: redhat
%admin ALL=(ALL) ALL
```

- 6.6. Regrese a la máquina `workstation` como el usuario `student`.

```
[sysadmin1@servera ~]$ exit
logout
[root@servera ~]# exit
logout
[student@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish users-group
```

Esto concluye la sección.

Administración de contraseñas de usuarios

Objetivos

Establecer una política de administración de contraseñas para los usuarios, y bloquear y desbloquear manualmente las cuentas de los usuarios.

Contraseñas ocultas y política de contraseñas

Originalmente, las contraseñas cifradas se almacenaban en el archivo /etc/passwd de lectura global. Se pensaba que esta ubicación era adecuada hasta que los ataques de diccionarios a contraseñas cifradas se volvieron frecuentes. Las contraseñas cifradas se trasladaron al archivo /etc/shadow, que solo el usuario root puede leer.

Al igual que el archivo /etc/passwd, cada usuario tiene una entrada con en el archivo /etc/shadow. Una entrada de ejemplo del archivo /etc/shadow tiene nueve campos separados por dos puntos:

```
[root@host ~]# cat /etc/shadow
...output omitted...
user03:$6$CSsXsd3rwghsdfarf:17933:0:99999:7:2:18113:
```

Cada campo de este bloque de código está separado por dos puntos:

- **user03** : Nombre de la cuenta de usuario.
- **\$6\$CSsXsd3rwghsdfarf** : Contraseña cifrada del usuario.
- **17933** : Días desde la época en que se cambió la contraseña por última vez, donde la época es 1970-01-01 en la zona horaria UTC.
- **0** : El número mínimo de días que deben transcurrir desde el último cambio de contraseña antes de que el usuario pueda volver a cambiarla.
- **99999** : El número máximo de días que pueden transcurrir sin un cambio de contraseña antes de que la contraseña caduque. Un campo vacío significa que la contraseña nunca caduca.
- **7** : Cantidad de días para advertir al usuario que su contraseña caducará.
- **2** : Cantidad de días sin actividad, comenzando con el día en que caducó la contraseña, antes de que la cuenta se bloquee automáticamente.
- **18113** : Día en que la cuenta caduca en días desde la época. Un campo vacío significa que la cuenta nunca caduca.
- Por lo general, el último campo está vacío y se reserva para su uso en el futuro.

Formato de una contraseña cifrada

El campo de contraseña cifrada almacena tres datos: el algoritmo de hash usado, el salt y el hash cifrado. Cada dato está delimitado por el signo del dólar (\$).

```
$6$CSsXcYG1L/4ZfHr/$2W6evvJahUfzfHpc9X.45Jc6H30E
```

- **6** : El algoritmo de hash usado para esta contraseña. Un 6 indica un hash SHA-512, el RHEL 9 predeterminado, un 1 indica MD5 y un 5 indica SHA-256.
- **CSsXcYG1L/4ZfHr/** : El valor aleatorio en uso para cifrar la contraseña; originalmente elegidos al azar.

- **2W6evvJahUfzfHpc9X.45Jc6H30E**: El hash cifrado de la contraseña del usuario; se combinan el salta y la contraseña cifrada, y se cifran para generar este hash de la contraseña.

El motivo principal para combinar un valor aleatorio con la contraseña es defenderse contra los ataques que usan listas de hash de contraseñas calculadas previamente. La adición de valores aleatorios cambia los hash resultantes, lo que permite que la lista previamente calculada sea inútil. Si un atacante obtiene una copia de un archivo `/etc/shadow` que usa valores aleatorios, necesita adivinar las contraseñas con fuerza bruta, lo que requiere más tiempo y esfuerzo.

Verificación de contraseña

Cuando un usuario intenta iniciar sesión, el sistema busca la entrada correspondiente al usuario en el archivo `/etc/shadow`, combina el valor aleatorio del usuario con la contraseña sin cifrar que se ingresó y los cifra usando la combinación de valor aleatorio y contraseña cifrada con 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.

Configuración de vigencia de contraseñas

En el siguiente diagrama, se indican los parámetros de vigencia de contraseñas relevantes que pueden ajustarse mediante el comando `chage` para implementar una política de vigencia de contraseñas. Observe que el nombre del comando es `chage` que significa "cambiar edad", y no debe confundirse con la palabra "cambiar".

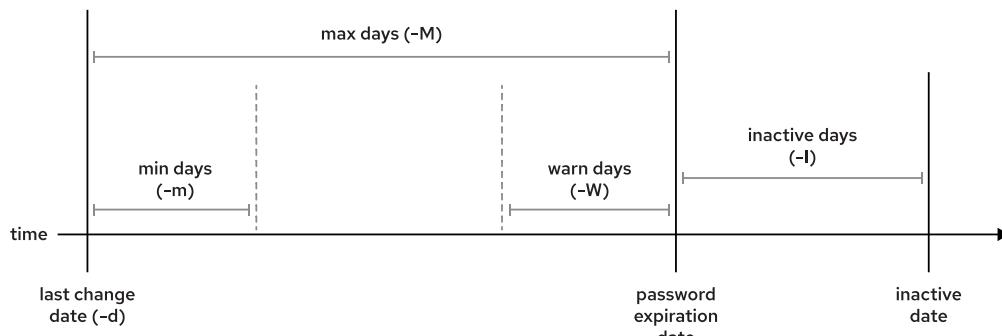


Figura 3.1: Parámetros de caducidad de la contraseña

En el siguiente ejemplo, se demuestra cómo el comando `chage` cambia la política de contraseña del usuario `sysadmin05`. El comando define una antigüedad mínima (`-m`) de cero días, una vigencia máxima (`-M`) de 90 días, un período de advertencia (`-W`) de 7 días y un período de inactividad (`-I`) de 14 días.

```
[root@host ~]# chage -m 0 -M 90 -W 7 -I 14 sysadmin05
```

Supongamos que administra las políticas de contraseña de usuario en un servidor de Red Hat. El usuario `cloudadmin10` es nuevo en el sistema y desea establecer una política de vigencia de contraseña personalizada. Desea establecer la caducidad de la cuenta en 30 días a partir de hoy, por lo que debe usar los siguientes comandos:

```
[root@host ~]# date +%F ①
2022-03-10
[root@host ~]# date -d "+30 days" +%F ②
2022-04-09
[root@host ~]# chage -E $(date -d "+30 days" +%F) cloudadmin10 ③
[root@host ~]# chage -l cloudadmin10 | grep "Account expires" ④
Account expires      : Apr 09, 2022
```

- ① Use el comando `date` para mostrar la fecha actual.
- ② Use el comando `date` para obtener la fecha dentro de 30 días.
- ③ Use el comando `chage` con la opción `-E` para cambiar la fecha de vencimiento para el usuario `cloudadmin10`.
- ④ Use el comando `chage` con la opción `-l` para mostrar la política de vigencia de la contraseña para el usuario `cloudadmin10`.

Después de unos días, observa en el archivo de registro `/var/log/secure` que el usuario `cloudadmin10` tiene un comportamiento extraño. El usuario intentó usar `sudo` para interactuar con archivos que pertenecen a otros usuarios. Usted sospecha que el usuario pudo haber dejado una sesión `ssh` abierta mientras trabajaba en otra máquina. Desea que el usuario `cloudadmin10` cambie la contraseña en el próximo inicio de sesión, por lo que debe usar el siguiente comando.

```
[root@host ~]# chage -d 0 cloudadmin10
```

La próxima vez que el usuario `cloudadmin10` inicie sesión, se le solicitará al usuario que cambie la contraseña.



nota

El comando `date` puede calcular una fecha en el futuro. La opción `-u` informa la hora en UTC.

```
[user01@host ~]$ date -d "+45 days" -u
Thu May 23 17:01:20 UTC 2019
```

Puede cambiar la configuración de vigencia de la contraseña predeterminada en el archivo `/etc/login.defs`. Las opciones `PASS_MAX_DAYS` y `PASS_MIN_DAYS` establecen la antigüedad máxima y mínima predeterminada de la contraseña, respectivamente. `PASS_WARN_AGE` define el período de advertencia predeterminado de la contraseña. Cualquier cambio en las políticas de vigencia de contraseñas predeterminadas afecta a los usuarios que se crean después del cambio. Los usuarios existentes siguen usando la configuración de vigencia de la contraseña anterior en lugar de las nuevas. Para obtener más información sobre el archivo `/etc/login.defs`, consulte el curso *Red Hat Security: Linux in Physical, Virtual, and Cloud* (RH415) y la página del manual `login.defs(5)`.

Restricción de acceso

Puede usar el comando `usermod` para modificar el vencimiento de la cuenta de un usuario. Por ejemplo, el comando `usermod` con la opción `-L` bloquea una cuenta de usuario y el usuario no puede iniciar sesión en el sistema.

```
[root@host ~]# usermod -L sysadmin03
[user01@host ~]$ su - sysadmin03
Password: redhat
su: Authentication failure
```

Si un usuario se va de la empresa en determinada fecha, puede bloquear la cuenta y determinar su caducidad con un único comando `usermod`. La fecha debe indicarse como la cantidad de días desde 1970-01-01 o en el formato AAAA-MM-DD. En el siguiente ejemplo, el comando `usermod` bloquea y expira el usuario `cloudadmin10` en 2022-08-14.

```
[root@host ~]# usermod -L -e 2022-08-14 cloudadmin10
```

Al bloquear una cuenta, evita que el usuario logre la autenticación con una contraseña en el sistema. Este método se recomienda para evitar el acceso a una cuenta por parte de un ex empleado de la empresa. Use el comando `usermod` con la opción `-U` para habilitar el acceso a la cuenta nuevamente.

La shell nologin

La shell `nologin` actúa como una shell de reemplazo para las cuentas de usuario que no están destinadas a iniciar sesión de forma interactiva en el sistema. Es una buena práctica de seguridad deshabilitar el inicio de sesión de una cuenta en el sistema, cuando la cuenta no lo requiere. Por ejemplo, un servidor de correo puede necesitar una cuenta para almacenar correos y una contraseña para que el usuario realice la autenticación con un cliente de correo 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` cierra la conexión.

```
[root@host ~]# usermod -s /sbin/nologin newapp
[root@host ~]# su - newapp
Last login: Wed Feb  6 17:03:06 IST 2019 on pts/0
This account is currently not available.
```



Importante

La shell `nologin` evita el uso interactivo del sistema, pero no evita todo el acceso. Los usuarios pueden, 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 si usan la contraseña del usuario para autenticarse.



Referencias

Páginas del manual: `chage(1)`, `usermod(8)`, `shadow(5)`, `crypt(3)` y `login.defs(5)`

► Ejercicio Guiado

Administración de contraseñas de usuarios

En este ejercicio, configurará políticas de contraseña para varios usuarios.

Resultados

- Forzar un cambio de contraseña cuando el usuario inicia sesión en el sistema por primera vez.
- Forzar un cambio de contraseña cada 90 días.
- Configurar la cuenta para que caduque 180 días a partir del día actual.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start users-password
```

Instrucciones

- 1. Desde `workstation`, abra una sesión de SSH en `student` como `servera`.

```
[student@workstation ~]$ ssh student@servera  
[student@servera ~]$
```

- 2. En `servera`, use el comando `usermod` para bloquear y desbloquear el usuario `operator1`.

- 2.1. Como usuario `student`, use los derechos administrativos para bloquear la cuenta `operator1`.

```
[student@servera ~]$ sudo usermod -L operator1  
[sudo] password for student: student
```

- 2.2. Intente iniciar sesión como `operator1`. Este comando debería fallar.

```
[student@servera ~]$ su - operator1  
Password: redhat  
su: Authentication failure
```

- 2.3. Desbloquee la cuenta `operator1`.

```
[student@servera ~]$ sudo usermod -U operator1
```

- 2.4. Intente iniciar sesión como **operator1** nuevamente. Esta vez, el comando debería ser exitoso.

```
[student@servera ~]$ su - operator1
Password: redhat
...output omitted...
[operator1@servera ~]$
```

- 2.5. Cierre sesión en la shell del usuario **operator1** para volver a la shell del usuario **student**.

```
[operator1@servera ~]$ exit
logout
```

- 3. Cambie la directiva de contraseña para el usuario **operator1** a fin de solicitar una contraseña nueva cada 90 días. Confirme que la vigencia de la contraseña se haya establecido correctamente.

- 3.1. Cambie al usuario **root**.

```
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

- 3.2. Establezca la vigencia máxima de la contraseña del usuario **operator1** en 90 días.

```
[root@servera ~]# chage -M 90 operator1
```

- 3.3. Verifique que la contraseña del usuario **operator1** caduque 90 días después de que se modifica.

```
[root@servera ~]# chage -l operator1
Last password change      : Mar 10, 2022
Password expires          : Jun 10, 2022
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
```

- 4. Fuerce un cambio de contraseña en el primer inicio de sesión en la cuenta de **operator1**.

```
[root@servera ~]# chage -d 0 operator1
```

- 5. Salga como el usuario **root** de la máquina **servera**.

```
[root@servera ~]# exit
logout
[student@servera ~]$
```

- 6. Inicie sesión como **operator1** y cambie la contraseña a **forsooth123**. Después de configurar la contraseña, vuelva a la shell del usuario **student**.
- 6.1. Inicie sesión como **operator1** y cambie la contraseña a **forsooth123** cuando se le solicite.

```
[student@servera ~]$ su - operator1
Password: redhat
You are required to change your password immediately (administrator enforced)
Current password: redhat
New password: forsooth123
Retype new password: forsooth123
...output omitted...
[operator1@servera ~]$
```

- 6.2. Salga de la shell del usuario **operator1** para volver al usuario **student** y luego cambie al usuario **root**.

```
[operator1@servera ~]$ exit
logout
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

- 7. Configure la cuenta de **operator1** para que caduque 180 días a partir del día actual.
- 7.1. Determine la fecha de vencimiento en 180 días. Use el formato %F con el comando **date** para obtener el valor exacto. Esta fecha devuelta es un ejemplo; use el valor en su sistema para los pasos posteriores a este.

```
[root@servera ~]# date -d "+180 days" +%F
2022-09-06
```

- 7.2. Configure la cuenta para que caduque en la fecha que se muestra en el paso anterior. Por ejemplo:

```
[root@servera ~]# chage -E 2022-09-06 operator1
```

- 7.3. Verifique que la fecha de vencimiento de la cuenta se haya establecido correctamente.

```
[root@servera ~]# chage -l operator1
Last password change      : Mar 10, 2022
Password expires          : Jun 10, 2022
Password inactive         : never
Account expires           : Sep 06, 2022
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
```

- 8. Establezca las contraseñas para que caduquen 180 días a partir de la fecha actual para todos los usuarios. Use los derechos administrativos para editar el archivo de configuración.
- 8.1. Establezca PASS_MAX_DAYS en 180 en /etc/login.defs. Use los derechos administrativos cuando abre el archivo con el editor de texto. Puede usar el comando vim /etc/login.defs para realizar este paso.

```
...output omitted...
# Password aging controls:
#
#      PASS_MAX_DAYS    Maximum number of days a password may be
#      used.
#      PASS_MIN_DAYS    Minimum number of days allowed between
#      password changes.
#      PASS_MIN_LEN     Minimum acceptable password length.
#      PASS_WARN_AGE    Number of days warning given before a
#      password expires.
#
PASS_MAX_DAYS 180
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
...output omitted...
```



Importante

La contraseña predeterminada y la configuración de caducidad de la cuenta aplican a los nuevos usuarios, pero no a los usuarios existentes.

- 8.2. Regrese al sistema `workstation` como el usuario `student`.

```
[root@servera ~]# exit
logout
[student@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish users-password
```

Esto concluye la sección.

► Trabajo de laboratorio

Administración de usuarios y grupos locales

En este trabajo de laboratorio, define una política de contraseña local predeterminada, crea un grupo secundario de tres usuarios, permite que el grupo use sudo para ejecutar comandos como `root` y modifica la política de contraseña de un usuario.

Resultados

- Establecer una política de vigencia de contraseña predeterminada de la contraseña del usuario local.
- Crear y usar un grupo secundario para nuevos usuarios.
- Crear tres nuevos usuarios con el nuevo grupo secundario.
- Establecer una contraseña inicial para los usuarios creados.
- Configurar los miembros del grupo secundario para usar el comando `sudo` para ejecutar cualquier comando como cualquier usuario.
- Establecer una política de vigencia de contraseña específica del usuario.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start users-review
```

Instrucciones

1. En la máquina `workstation`, abra una sesión de SSH en la máquina `serverb` como el usuario `student` y cambie al usuario `root`.
2. En la máquina `serverb`, asegúrese de que los usuarios creados recientemente tengan contraseñas que se deben cambiar cada 30 días.
3. Cree el grupo `consultants` con un GID de 35000.
4. Configure los derechos administrativos para permitir que todos los miembros del grupo `consultants` ejecuten cualquier comando como cualquier usuario.
5. Cree los usuarios `consultant1`, `consultant2` y `consultant3` con el grupo `consultants` como su grupo secundario.
6. Establezca las contraseñas `consultant1`, `consultant2` y `consultant3` como `redhat`.
7. Configure las cuentas `consultant1`, `consultant2` y `consultant3` para que vengan en 90 días a partir del día actual.
8. Cambie la directiva de contraseña para la cuenta `consultant2` a fin de solicitar una contraseña nueva cada 15 días.

9. Además, fuerce a los usuarios `consultant1`, `consultant2` y `consultant3` a cambiar sus contraseñas en el primer inicio de sesión.

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `Lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade users-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `Lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish users-review
```

Esto concluye la sección.

► Solución

Administración de usuarios y grupos locales

En este trabajo de laboratorio, define una política de contraseña local predeterminada, crea un grupo secundario de tres usuarios, permite que el grupo use sudo para ejecutar comandos como `root` y modifica la política de contraseña de un usuario.

Resultados

- Establecer una política de vigencia de contraseña predeterminada de la contraseña del usuario local.
- Crear y usar un grupo secundario para nuevos usuarios.
- Crear tres nuevos usuarios con el nuevo grupo secundario.
- Establecer una contraseña inicial para los usuarios creados.
- Configurar los miembros del grupo secundario para usar el comando sudo para ejecutar cualquier comando como cualquier usuario.
- Establecer una política de vigencia de contraseña específica del usuario.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start users-review
```

Instrucciones

1. En la máquina `workstation`, abra una sesión de SSH en la máquina `serverb` como el usuario `student` y cambie al usuario `root`.

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
[student@serverb ~]$ sudo -i
[sudo] password for student: student
[root@serverb ~]#
```

2. En la máquina `serverb`, asegúrese de que los usuarios creados recientemente tengan contraseñas que se deben cambiar cada 30 días.
 - 2.1. Establezca `PASS_MAX_DAYS` en 30 en el archivo `/etc/login.defs`. Use los derechos administrativos al abrir el archivo con el editor de texto. Puede usar el comando `vim /etc/login.defs` para realizar este paso.

```

...output omitted...
# Password aging controls:
#
#      PASS_MAX_DAYS   Maximum number of days a password may be
#      used.
#      PASS_MIN_DAYS   Minimum number of days allowed between
#      password changes.
#      PASS_MIN_LEN     Minimum acceptable password length.
#      PASS_WARN_AGE    Number of days warning given before a
#      password expires.
#
PASS_MAX_DAYS 30
PASS_MIN_DAYS  0
PASS_WARN_AGE  7
...output omitted...

```

- Cree el grupo **consultants** con un GID de 35000.

```
[root@serverb ~]# groupadd -g 35000 consultants
```

- Configure los derechos administrativos para permitir que todos los miembros del grupo **consultants** ejecuten cualquier comando como cualquier usuario.
 - Cree el archivo **/etc/sudoers.d/consultants** y agréguele el siguiente contenido. Puede usar el comando **vim /etc/sudoers.d/consultants** para realizar este paso.

```
%consultants  ALL=(ALL) ALL
```

- Cree los usuarios **consultant1**, **consultant2** y **consultant3** con el grupo **consultants** como su grupo secundario.

```
[root@serverb ~]# useradd -G consultants consultant1
[root@serverb ~]# useradd -G consultants consultant2
[root@serverb ~]# useradd -G consultants consultant3
```

- Establezca las contraseñas **consultant1**, **consultant2** y **consultant3** como **redhat**.

```
[root@serverb ~]# passwd consultant1
Changing password for user consultant1.
New password: redhat
BAD PASSWORD: The password is shorter than 8 characters
Retype new password: redhat
passwd: all authentication tokens updated successfully.
[root@serverb ~]# passwd consultant2
Changing password for user consultant2.
New password: redhat
BAD PASSWORD: The password is shorter than 8 characters
Retype new password: redhat
passwd: all authentication tokens updated successfully
[root@serverb ~]# passwd consultant3
Changing password for user consultant3.
```

```
New password: redhat
BAD PASSWORD: The password is shorter than 8 characters
Retype new password: redhat
passwd: all authentication tokens updated successfully
```

7. Configure las cuentas `consultant1`, `consultant2` y `consultant3` para que venzan en 90 días a partir del día actual.

- 7.1. Determine la fecha de vencimiento en 90 días. Esta fecha devuelta es un ejemplo; el valor que ve, para usar en el siguiente paso, se basa en la fecha y hora actuales en su sistema.

```
[root@serverb ~]# date -d "+90 days" +%F
2022-06-08
```

- 7.2. Configure la fecha de vencimiento de las cuentas `consultant1`, `consultant2` y `consultant3` con el mismo valor determinado en el paso anterior. Por ejemplo:

```
[root@serverb ~]# chage -E 2022-06-08 consultant1
[root@serverb ~]# chage -E 2022-06-08 consultant2
[root@serverb ~]# chage -E 2022-06-08 consultant3
```

8. Cambie la directiva de contraseña para la cuenta `consultant2` a fin de solicitar una contraseña nueva cada 15 días.

```
[root@serverb ~]# chage -M 15 consultant2
```

9. Además, fuerce a los usuarios `consultant1`, `consultant2` y `consultant3` a cambiar sus contraseñas en el primer inicio de sesión.

- 9.1. Establezca el último día del cambio de contraseña en 0 para que los usuarios deban cambiar la contraseña cuando inicien sesión en el sistema por primera vez.

```
[root@serverb ~]# chage -d 0 consultant1
[root@serverb ~]# chage -d 0 consultant2
[root@serverb ~]# chage -d 0 consultant3
```

- 9.2. Regrese al sistema `workstation` como el usuario `student`.

```
[root@serverb ~]# exit
logout
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@workstation ~]$
```

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade users-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish users-review
```

Esto concluye la sección.

Resumen

- Los tipos de cuentas de usuario en Linux son: el superusuario, los usuarios del sistema y los usuarios normales.
- Un usuario tiene un grupo primario y puede ser miembro de grupos secundarios.
- Los tres archivos críticos que contienen información de usuarios y grupos son `/etc/passwd`, `/etc/group` y `/etc/shadow`.
- Puede ejecutar comandos como el superusuario con los comandos `su` y `sudo`.
- Los comandos `useradd`, `usermod` y `userdel` administran usuarios.
- Los comandos `groupadd`, `groupmod` y `groupdel` administran grupos.
- El comando `passwd` administra las contraseñas de los usuarios.
- El comando `chage` se puede usar para configurar y ver la configuración de caducidad de la contraseña de los usuarios.

capítulo 4

Control de acceso a los archivos

Meta

Configurar los permisos del sistema de archivos Linux en los archivos e interpretar los efectos de seguridad de los distintos parámetros de configuración de permisos.

Objetivos

- Cambiar los permisos y la propiedad de los archivos con las herramientas de línea de comandos.
- Controlar los permisos predeterminados de los archivos creados por los usuarios, explicar el efecto de los permisos especiales y usar permisos especiales y permisos predeterminados para configurar el propietario del grupo de archivos creados en un directorio.

Secciones

- Administración de los permisos del sistema de archivos de la línea de comandos (y ejercicio guiado)
- Administración de permisos predeterminados y acceso a archivos (y ejercicio guiado)

Trabajo de laboratorio

- Control de acceso a los archivos

Administración de permisos del sistema de archivos desde la línea de comandos

Objetivos

Cambiar los permisos y la propiedad de los archivos con las herramientas de línea de comandos.

Cambio de permisos de archivos y directorios

El comando `chmod` cambia los permisos de archivo y directorio desde la línea de comandos. El comando `chmod` puede interpretarse como "cambiar modo", ya que el *modo* de un archivo es otro nombre para los permisos de archivo. El comando `chmod` tiene una instrucción de permiso seguida de una lista de archivos o directorios para cambio. Puede establecer la instrucción de permiso de forma simbólica o en notación octal (numérica).

Cambiar los permisos con el método simbólico

Use el comando `chmod` para modificar los permisos de archivos y directorios. El siguiente ejemplo puede ayudarlo a comprender el uso del comando `chmod`:

```
chmod Who/What/Which file|directory
```

Quién es la clase de usuario, como se muestra en la siguiente tabla. Si no proporciona una clase de usuario, el comando `chmod` usa el grupo `all` como predeterminado.

Quién	Conjunto	Descripción
u	usuario	El propietario del archivo.
g	grupo	Miembro del grupo del archivo.
o	otros	Usuarios que no son el propietario del archivo ni miembros del grupo del archivo.
a	todos	Los tres grupos anteriores.

Qué es el operador que modifica a *Cuál*, como se muestra en la siguiente tabla.

Qué	Operación	Descripción
+	agregar	Agrega los permisos al archivo.
-	borrar	Borra los permisos del archivo.
=	establecer exactamente	Establece exactamente los permisos proporcionados para el archivo.

Cuál es el modo, y especifica los permisos para los archivos o directorios, como se muestra en la siguiente tabla.

Cuál	Modo	Descripción
r	lectura	Acceso de lectura al archivo. Enumeración del acceso al directorio.
w	escritura	Permisos de escritura en el archivo o directorio.
x	ejecución	Ejecución de los permisos del archivo. Permite ingresar al directorio y acceder a archivos y subdirectorios dentro del directorio.
X	ejecución especial	Permisos de ejecución para un directorio, o permisos de ejecución para un archivo si tiene al menos uno de los bits de ejecución establecido.

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 debe establecer un grupo completamente nuevo de permisos. En su lugar, puede cambiar uno o más permisos existentes. Use los caracteres más (+) o menos (-) para agregar o eliminar permisos, respectivamente, o use el carácter igual (=) para reemplazar todo el conjunto de un grupo de permisos.

Una sola letra representa los permisos en sí: r para lectura, w para escritura y x para ejecución. Puede usar una mayúscula X como indicador de permiso para agregar permisos de ejecución solo si el archivo es un directorio o si la ejecución ya está configurada para usuario, grupo u otro.

En la siguiente lista, se muestran algunos ejemplos para cambiar los permisos con el método simbólico:

Elimine el permiso de lectura y escritura para el grupo y otros en el archivo `document.pdf`:

```
[user@host ~]$ chmod go-rw document.pdf
```

Agregue un permiso de ejecución para todos en el archivo `myscript.sh`:

```
[user@host ~]$ chmod a+x myscript.sh
```

Puede usar el comando `chmod` con la opción -R para establecer permisos de manera recursiva en los archivos, en todo el árbol de directorios. Por ejemplo, el siguiente comando agrega de manera recursiva permisos de lectura, escritura y ejecución para los miembros del directorio `myfolder` y los archivos y directorios dentro de este.

```
[user@host ~]$ chmod -R g+rwx /home/user/myfolder
```

También puede usar el comando `chmod` con la opción -R y la opción -X para establecer permisos simbólicamente. El comando `chmod` con la opción X le permite 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. Sin embargo, tenga cuidado con la opción X, porque si un archivo tiene un permiso de ejecución establecido, la opción X establecerá el permiso de ejecución especificado en ese archivo también.

Por ejemplo, el siguiente comando establece de manera recursiva el acceso de lectura y de escritura en el directorio `demodir` y todos sus procesos secundarios para el propietario del grupo,

pero solo aplica permisos de ejecución de grupo a directorios y archivos que ya tienen permisos de ejecución establecidos para usuario, grupo u otros.

```
[root@host opt]# chmod -R g+rwx demodir
```

Cómo cambiar los permisos con el método octal

Puede usar el comando `chmod` para cambiar los permisos de archivo con el método octal en lugar del método simbólico. En el siguiente ejemplo, el carácter # representa un dígito.

```
chmod ### file|directory
```

Al usar el método octal, puede representar los permisos con un número *octal* de tres dígitos (o cuatro, al establecer permisos avanzados). Un octal de un único dígito puede representar cualquier valor de 0 a 7.

En la representación de permisos octal de tres dígitos, cada dígito representa un nivel de acceso, de izquierda a derecha: usuario, grupo y otros. Para determinar cada dígito:

- Comience con 0.
- Si desea agregar permisos de lectura para este nivel de acceso, agregue 4.
- Si desea agregar permisos de escritura, agregue 2.
- Si desea agregar permisos de ejecución, agregue 1.

En el siguiente diagrama, se ilustra cómo los sistemas interpretan el valor de permiso octal 644.

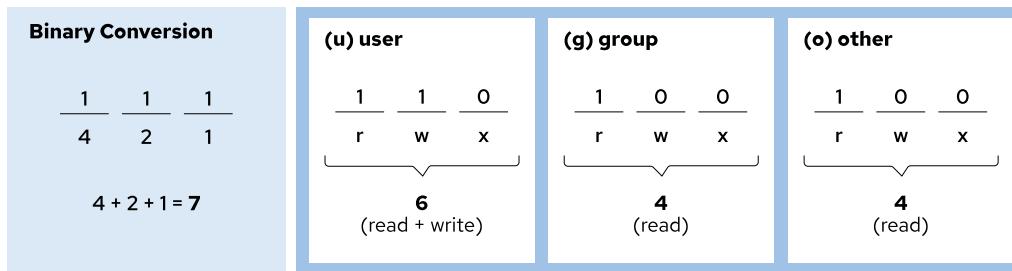


Figura 4.1: Representación visual del método octal

Los administradores experimentados a menudo usan permisos octales porque son más fáciles de implementar en archivos únicos o coincidentes, y aún proporcionan un control total de permisos.

En la siguiente lista, se muestran algunos ejemplos para cambiar los permisos con el método octal:

Establezca permisos de lectura y escritura para el usuario, permiso de lectura para el grupo y otros en el archivo `sample.txt`:

```
[user@host ~]$ chmod 644 sample.txt
```

Establezca permisos de lectura, escritura y ejecución para usuario, permisos de lectura y ejecución para grupo y ningún permiso para otros en el directorio `sampledir`:

```
[user@host ~]$ chmod 750 sampledir
```

Cambio de la propiedad de grupo o de usuario de un archivo o directorio

El usuario es propietario de un archivo que crea. De manera predeterminada, los archivos nuevos son propiedad del grupo, que es el grupo principal del usuario que crea el archivo. En Red Hat Enterprise Linux, el grupo principal de un usuario suele ser un grupo privado que solamente tiene a ese usuario como miembro. Para otorgar acceso a un archivo según la membresía de grupo, es posible que sea necesario cambiar el grupo que es propietario del archivo.

Solo el usuario `root` puede cambiar el usuario que es propietario de un archivo. Sin embargo, el propietario del archivo y el usuario `root` pueden establecer la propiedad del grupo. El usuario `root` puede otorgar propiedad del archivo a cualquier grupo, pero solo los usuarios regulares pueden cambiar la propiedad del grupo del archivo si son miembros del grupo de destino.

Puede cambiar la propiedad del archivo con el comando `chown` (cambiar propietario). Por ejemplo, para otorgarle propiedad del archivo `app.conf` al usuario `student`, use el siguiente comando:

```
[root@host ~]# chown student app.conf
```

El comando `chown` con la opción `-R` cambia recursivamente la propiedad de un árbol de directorios completo. El siguiente comando otorga propiedad del directorio `Pictures` y de todos los archivos y subdirectorios incluidos en él al usuario `student`:

```
[root@host ~]# chown -R student Pictures
```

El comando `chown` también se puede usar para cambiar el propietario del grupo de un archivo, anteponiendo el nombre del grupo con dos puntos (`:`). Por ejemplo, el siguiente comando cambia la propiedad del grupo del directorio `Pictures` a `admins`:

```
[root@host ~]# chown :admins Pictures
```

Puede usar el comando `chown` para cambiar el propietario y el grupo al mismo tiempo. Para ello, puede usar la sintaxis `propietario:grupo`. Por ejemplo, para cambiar la propiedad del directorio `Pictures` al usuario `visitor` y el grupo `guests`, use el siguiente comando:

```
[root@host ~]# chown visitor:guests Pictures
```

En lugar de usar el comando `chown`, algunos usuarios cambian la propiedad del grupo usando el comando `chgrp`. Este comando funciona igual que `chown`, excepto que solo se usa para cambiar la propiedad del grupo, y no es necesario colocar los dos puntos (`:`) antes del nombre del grupo.



Importante

Puede encontrar una sintaxis alternativa `chown` que separa al propietario y al grupo con un punto en lugar de dos puntos:

```
[root@host ~]# chown owner.group filename
```

Red Hat recomienda no usar esta sintaxis y usar siempre dos puntos. Debido a que un punto es un carácter válido en un nombre de usuario, un comando `chown` puede malinterpretar su intención. El comando puede interpretar el usuario y el grupo como un nombre de archivo. En su lugar, solo use dos puntos cuando configure el usuario y el grupo al mismo tiempo.



Referencias

Páginas del manual: `ls(1)`, `chmod(1)`, `chown(1)` y `chgrp(1)`

► Ejercicio Guiado

Administración de permisos del sistema de archivos desde la línea de comandos

En este ejercicio, usa los permisos del sistema de archivos para crear un directorio en el que todos los miembros de un grupo particular puedan agregar y eliminar archivos.

Resultados

- Crear un directorio de colaboración al que puedan acceder todos los miembros de un grupo en particular.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start perms-cli
```

Instrucciones

- 1. En `workstation`, inicie sesión en `servera` como el usuario `student` y cambie al usuario `root`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ sudo -i
Password: student
[root@servera ~]#
```

- 2. Cree el directorio `/home/consultants`.

```
[root@servera ~]# mkdir /home/consultants
```

- 3. Cambie la propiedad del directorio `consultants` a `consultants`.

```
[root@servera ~]# chown :consultants /home/consultants
```

- 4. Asegúrese de que los permisos del grupo `consultants` permitan a los miembros del grupo crear archivos en el directorio `/home/consultants` y eliminarlos de este. Use el método simbólico para establecer los permisos adecuados.

Los permisos deben impedir que otros accedan a los archivos. Use el método octal para establecer los permisos adecuados.

capítulo 4 | Control de acceso a los archivos

- 4.1. Asegúrese de que los permisos del grupo `consultants` permitan a los miembros del grupo crear archivos en el directorio `/home/consultants` y eliminarlos de este. Tenga en cuenta que el grupo `consultants` actualmente no tiene permiso de escritura.

```
[root@servera ~]# ls -ld /home/consultants
drwxr-xr-x. 2 root     consultants   6 Mar  1 12:08 /home/consultants
```

- 4.2. Agregue permiso de escritura al grupo `consultants`.

```
[root@servera ~]# chmod g+w /home/consultants
[root@servera ~]# ls -ld /home/consultants
drwxrwxr-x. 2 root consultants 6 Mar  1 13:21 /home/consultants
```

- 4.3. Impida que otros accedan a los archivos del directorio `/home/consultants`.

```
[root@servera ~]# chmod 770 /home/consultants
[root@servera ~]# ls -ld /home/consultants
drwxrwx---. 2 root consultants 6 Mar  1 12:08 /home/consultants/
```

- 5. Salga de la shell `root` y cambie al usuario `consultant1`. La contraseña es `redhat`.

```
[root@servera ~]# exit
logout
[student@servera ~]$ su - consultant1
Password: redhat
[consultant1@servera ~]$
```

- 6. Diríjase al directorio `/home/consultants` y cree un archivo llamado `consultant1.txt`.

- 6.1. Cambie al directorio `/home/consultants`.

```
[consultant1@servera ~]$ cd /home/consultants
```

- 6.2. Cree un archivo vacío denominado `consultant1.txt`.

```
[consultant1@servera consultants]$ touch consultant1.txt
```

- 7. Enumere las propiedades de grupo y de usuario predeterminadas del nuevo archivo y sus permisos.

```
[consultant1@servera consultants]$ ls -l consultant1.txt
-rw-rw-r--. 1 consultant1 consultant1 0 Mar  1 12:53 consultant1.txt
```

- 8. Asegúrese de que todos los miembros del grupo `consultants` puedan editar el archivo `consultant1.txt`. Cambie la propiedad del grupo del archivo `consultant1.txt` a `consultants`.

- 8.1. Use el comando `chown` para cambiar la propiedad del grupo del archivo `consultant1.txt` a `consultants`.

```
[consultant1@servera consultants]$ chown :consultants consultant1.txt
```

- 8.2. Enumere la nueva propiedad del archivo `consultant1.txt`.

```
[consultant1@servera consultants]$ ls -l consultant1.txt  
-rw-rw-r-- 1 consultant1 consultants 0 Mar 1 12:53 consultant1.txt
```

- 9. Salga de la shell y cambie al usuario `consultant2`. La contraseña es `redhat`.

```
[consultant1@servera consultants]$ exit  
logout  
[student@servera ~]$ su - consultant2  
Password: redhat  
[consultant2@servera ~]$
```

- 10. Diríjase al directorio `/home/consultants`. Asegúrese de que el usuario `consultant2` puede agregar contenido al archivo `consultant1.txt`.

- 10.1. Cambie al directorio `/home/consultants`. Agregue `text` al archivo `consultant1.txt`.

```
[consultant2@servera ~]$ cd /home/consultants/  
[consultant2@servera consultants]$ echo "text" >> consultant1.txt
```

- 10.2. Verifique que el texto esté presente en el archivo `consultant1.txt`.

```
[consultant2@servera consultants]$ cat consultant1.txt  
text
```

- 10.3. Regrese al sistema `workstation` como el usuario `student`.

```
[consultant2@servera consultants]$ exit  
logout  
[student@servera ~]$ exit  
logout  
Connection to servera closed.  
[student@workstation ~]$
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish perms-cli
```

Esto concluye la sección.

Administración de permisos predeterminados y acceso a archivos

Objetivos

Controlar los permisos predeterminados de los archivos creados por los usuarios, explicar el efecto de los permisos especiales y usar permisos especiales y permisos predeterminados para configurar el propietario del grupo de archivos creados en un directorio.

Permisos especiales

Los *permisos especiales* son un cuarto tipo de permiso, además del usuario básico, grupo y otros tipos. Como su nombre lo indica, estos permisos especiales proporcionan funciones adicionales relacionadas con el acceso más allá de lo que permiten los tipos de permisos básicos. En esta sección, se describe el impacto de los permisos especiales, que se resumen en la siguiente tabla.

Efectos de los permisos especiales en archivos y directorios

Permiso	Efecto en los archivos	Efecto en los directorios
u+s (suid)	El archivo se ejecuta como el usuario propietario del archivo, no como el usuario que lo ejecutó.	No hay efectos.
g+s (sgid)	El archivo se ejecuta como el grupo propietario.	Los archivos creados 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 acceso de escritura 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.

El permiso *setuid* en un archivo ejecutable significa que los comandos se ejecutan como el usuario que es propietario de ese archivo, en lugar de como el usuario que ejecutó el comando. Un ejemplo de este caso es el comando `passwd`:

```
[user@host ~]$ ls -l /usr/bin/passwd
-rwsr-xr-x. 1 root root 35504 Jul 16 2010 /usr/bin/passwd
```

En una larga lista, puede identificar los permisos *setuid* con una minúscula s, donde normalmente esperaría ver el carácter x (el propietario ejecuta los permisos). Si el propietario no posee permisos de ejecución, este carácter será reemplazado por una S mayúscula.

El permiso especial *setgid* en un directorio significa que los archivos creados en el directorio heredarán la propiedad de grupos del directorio, en lugar de heredarla del usuario que la creó. Esta función generalmente se usa en directorios colaborativos grupales para poder cambiar

capítulo 4 | Control de acceso a los archivos

automáticamente un archivo del grupo privado predeterminado al grupo compartido, o si los archivos de un directorio deben pertenecer siempre a un grupo específico. Un ejemplo de este comportamiento es el directorio `/run/log/journal`:

```
[user@host ~]$ ls -ld /run/log/journal  
drwxr-sr-x. 3 root systemd-journal 60 May 18 09:15 /run/log/journal
```

Si `setgid` se establece en un archivo ejecutable, significa que los comandos se ejecutan como el grupo que es propietario del archivo, no como el usuario que ejecutó el comando. Esta condición es similar a la forma en que funciona `setuid`. Un ejemplo de este caso es el comando `locate`:

```
[user@host ~]$ ls -ld /usr/bin/locate  
-rwx--s--x. 1 root slocate 47128 Aug 12 17:17 /usr/bin/locate
```

En una larga lista, puede identificar los permisos `setgid` con una s minúscula, donde normalmente esperaría ver el carácter x (el grupo ejecuta los permisos). Si el grupo no posee permisos de ejecución, este carácter será reemplazado por una S mayúscula.

Finalmente, el *sticky bit* para un directorio establece una restricción especial en la eliminación de archivos. Solo el propietario del archivo (y el usuario `root`) puede borrar archivos dentro del directorio. Un ejemplo es el directorio `/tmp`:

```
[user@host ~]$ ls -ld /tmp  
drwxrwxrwt. 39 root root 4096 Feb 8 20:52 /tmp
```

En una larga lista, puede identificar los permisos sticky con una minúscula t, donde normalmente esperaría ver el carácter x (otros ejecutan los permisos). Si otros no tienen permisos de ejecución, este carácter será reemplazado por una T mayúscula.

Establecer permisos especiales

- **Simbólico:** `setuid = u+s; setgid = g+s; sticky = o+t`
- **Octal:** En el cuarto dígito anterior añadido; `setuid = 4; setgid = 2; sticky = 1`

Ejemplos de permisos especiales Agregue el bit `setgid` en el directorio `example` usando el método simbólico:

```
[user@host ~]# chmod g+s example
```

Elimine el bit `setuid` en el directorio `example` mediante el uso del método simbólico:

```
[user@host ~]# chmod u-s example
```

Establezca el bit `setgid` y agregue permisos de lectura/escritura/ejecución para el usuario y grupo, sin acceso para otros, en el directorio `example` con el método octal:

```
[user@host ~]# chmod 2770 example
```

Elimine el bit `setgid` y agregue permisos de lectura/escritura/ejecución para el usuario y grupo, sin acceso para otros, en el directorio `example` con el método octal: Tenga en cuenta que debe agregar un 0 adicional al comienzo del valor de permisos al eliminar permisos especiales mediante el uso del método octal:

```
[user@host ~]# chmod 00770 example
```

Permisos predeterminados de archivos

Al crearse, se asignan permisos iniciales a un archivo. Dos cosas afectan estos permisos iniciales. En primer lugar, si está creando un archivo o directorio regulares. El segundo es el *umask* actual, que significa máscara de creación de archivos de usuario.

Si crea un directorio, sus permisos octales iniciales son 0777 (drwxrwxrwx). Si crea un archivo regular, sus permisos octales iniciales son 0666 (-rw-rw-rw-). Siempre debe agregar explícitamente el permiso de ejecución a un archivo regular. Este paso dificulta que un atacante ponga en peligro un sistema, cree un archivo malicioso y lo ejecute.

Además, la sesión de shell establece un umask para restringir aún más los permisos iniciales de un archivo. El umask es una máscara de bits octal usada 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 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 0077 borra los permisos de todo el grupo y de otros de los archivos creados recientemente.

El comando *umask* sin argumentos muestra el valor actual del umask de shell:

```
[user@host ~]$ umask  
0002
```

Use el comando *umask* con un argumento octal único para cambiar el umask de la shell actual. El argumento debe ser un valor octal que se corresponda con el nuevo valor del umask. Puede omitir los ceros iniciales en el umask.

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 anular los valores predeterminados del sistema en sus archivos *.bash_profile* o *.bashrc* en sus directorios de inicio.

Efecto de la utilidad umask en los permisos

En el siguiente ejemplo, se explica cómo el umask afecta los permisos de los archivos y directorios. Observe los permisos predeterminados de umask para archivos y directorios en la shell actual.

Si crea un archivo regular, sus permisos octales iniciales son 0666 (000 110 110 110, en representación binaria). Luego, la umask 0002 (000 000 000 010) deshabilita el bit de permiso de escritura para otros. Tanto el propietario como el grupo tienen permiso de lectura y escritura en los archivos, y otros tienen permiso de lectura (000 110 110 100).

	Symbolic	Numeric octal	Numeric binary
Initial file permissions	rw-rw-rw-	0666	000 110 110 110
umask	-----w-	0002	000 000 000 010
Resulting file permissions	rw-rw-r--	0664	000 110 110 100

Figura 4.2: Ejemplo de cálculo de umask en un archivo

```
[user@host ~]$ umask
0002
[user@host ~]$ touch default.txt
[user@host ~]$ ls -l default.txt
-rw-rw-r--. 1 user user 0 May  9 01:54 default.txt
```

Si crea un directorio, sus permisos octales iniciales son 0777 (000 111 111 111). Luego, el umask 0002 (000 000 000 010) deshabilita el bit de permiso de escritura para otros. Tanto el propietario como el grupo tienen permiso de lectura, escritura y ejecución en los directorios, y otros tienen permiso de lectura y ejecución (000 111 111 101).

	Symbolic	Numeric octal	Numeric binary
Initial directory permissions	rwxrwxrwx	0777	000 111 111 111
umask	-----w-	0002	000 000 000 010
Resulting directory permissions	rwxrwxr-x	0775	000 111 111 101

Figura 4.3: Ejemplo de cálculo de umask en un directorio

```
[user@host ~]$ umask
0002
[user@host ~]$ mkdir default
[user@host ~]$ ls -ld default
drwxrwxr-x. 2 user user 0 May  9 01:54 default
```

Al establecer el valor de umask en 0, los permisos del archivo para otros cambian de lectura a lectura y escritura. Los permisos del directorio para otros cambian de lectura y ejecución a lectura, escritura y ejecución.

```
[user@host ~]$ umask 0
[user@host ~]$ touch zero.txt
[user@host ~]$ ls -l zero.txt
-rw-rw-rw-. 1 user user 0 May  9 01:54 zero.txt
[user@host ~]$ mkdir zero
[user@host ~]$ ls -ld zero
drwxrwxrwx. 2 user user 0 May  9 01:54 zero
```

Para enmascarar todos los permisos de archivos y directorios para otros, establezca el valor de umask en 007.

```
[user@host ~]$ umask 007
[user@host ~]$ touch seven.txt
[user@host ~]$ ls -l seven.txt
-rw-rw----. 1 user user 0 May  9 01:55 seven.txt
[user@host ~]$ mkdir seven
[user@host ~]$ ls -ld seven
drwxrwx---. 2 user user 0 May  9 01:54 seven
```

Un umask de 027 garantiza que los nuevos archivos tengan permisos de lectura y escritura para el usuario y permisos de lectura para el grupo. Los nuevos directorios tienen acceso de lectura y escritura para el grupo y no tienen permisos para otros.

```
[user@host ~]$ umask 027
[user@host ~]$ touch two-seven.txt
[user@host ~]$ ls -l two-seven.txt
-rw-r-----. 1 user user 0 May  9 01:55 two-seven.txt
[user@host ~]$ mkdir two-seven
[user@host ~]$ ls -ld two-seven
drwxr-x---. 2 user user 0 May  9 01:54 two-seven
```

Los scripts de inicio de shell establecen el umask predeterminado para usuarios. De manera predeterminada, si la UID de su cuenta es 200 o más y su nombre de usuario y nombre de grupo principal son los mismos, se le asignará un umask de 002. De lo contrario, el umask es 022.

El usuario root puede cambiar el umask predeterminado agregando un script de inicio de shell `local-umask.sh` en el directorio `/etc/profile.d/`. En el siguiente ejemplo, se muestra el archivo `local-umask.sh`:

```
[root@host ~]# cat /etc/profile.d/local-umask.sh
# Overrides default umask configuration asda sda
if [ $UID -gt 199 ] && [ "`id -gn`" = "`id -un`" ]; then
    umask 007
else
    umask 022
fi
```

En el ejemplo anterior, se establece el umask en 007 para los usuarios con una UID mayor que 199 y con un nombre de usuario y un nombre de grupo primario iguales, y en 022 para todos los demás. Si solo quiere establecer el umask para todos en 022, puede crear ese archivo con el siguiente contenido:

```
# Overrides default umask configuration
umask 022
```

El umask actual de un intérprete de comandos se aplica hasta que cierre la sesión del intérprete de comandos y vuelva a iniciarla.



Referencias

Páginas del manual: `bash(1)`, `ls(1)`, `chmod(1)` y `umask(1)`

► Ejercicio Guiado

Administración de permisos predeterminados y acceso a archivos

En este ejercicio, controlará los permisos de los archivos creados en un directorio mediante el uso de la configuración de umask y el permiso setgid.

Resultados

- Crear un directorio compartido en el que el grupo `operators` pasa automáticamente a ser propietario de nuevos archivos.
- Probar diversos valores de configuración de umask.
- Ajustar los permisos predeterminados para usuarios específicos.
- Verificar su ajuste.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start perms-default
```

Instrucciones

- 1. Inicie sesión en el sistema `servera` como el usuario `student`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

- 2. Cambie al usuario `operator1` con `redhat` como contraseña.

```
[student@servera ~]$ su - operator1
Password: redhat
[operator1@servera ~]$
```

- 3. Mencione el valor de umask predeterminado del usuario `operator1`.

```
[operator1@servera ~]$ umask
0002
```

- 4. Cree un directorio `/tmp/shared`. En el directorio `/tmp/shared`, cree un archivo `defaults`. Observe los permisos predeterminados.

capítulo 4 | Control de acceso a los archivos

- 4.1. Cree el directorio /tmp/shared. Enumere los permisos del nuevo directorio.

```
[operator1@servera ~]$ mkdir /tmp/shared  
[operator1@servera ~]$ ls -ld /tmp/shared  
drwxrwxr-x. 2 operator1 operator1 6 Feb 4 14:06 /tmp/shared
```

- 4.2. Cree un archivo defaults en el directorio /tmp/shared.

```
[operator1@servera ~]$ touch /tmp/shared/defaults
```

- 4.3. Enumere los permisos del nuevo archivo.

```
[operator1@servera ~]$ ls -l /tmp/shared/defaults  
-rw-rw-r--. 1 operator1 operator1 0 Feb 4 14:09 /tmp/shared/defaults
```

- 5. Cambie la propiedad del directorio /tmp/shared al grupo operators. Confirme la nueva propiedad y los permisos.

- 5.1. Cambie la propiedad del directorio /tmp/shared al grupo operators.

```
[operator1@servera ~]$ chown :operators /tmp/shared
```

- 5.2. Enumere los permisos del directorio /tmp/shared.

```
[operator1@servera ~]$ ls -ld /tmp/shared  
drwxrwxr-x. 2 operator1 operators 22 Feb 4 14:09 /tmp/shared
```

- 5.3. Cree un archivo group en el directorio /tmp/shared. Enumere los permisos del archivo.

```
[operator1@servera ~]$ touch /tmp/shared/group  
[operator1@servera ~]$ ls -l /tmp/shared/group  
-rw-rw-r--. 1 operator1 operator1 0 Feb 4 17:00 /tmp/shared/group
```

**nota**

El propietario del grupo del archivo /tmp/shared/group no es operators, sino operator1.

- 6. Asegúrese de que los archivos creados en el directorio /tmp/shared sean propiedad del grupo operators.

- 6.1. Establezca el ID de grupo al grupo operators para el directorio /tmp/shared.

```
[operator1@servera ~]$ chmod g+s /tmp/shared
```

- 6.2. Cree un archivo ops_db.txt en el directorio /tmp/shared.

```
[operator1@servera ~]$ touch /tmp/shared/ops_db.txt
```

6.3. Verifique que el grupo `operators` es el propietario del grupo para el nuevo archivo.

```
[operator1@servera ~]$ ls -l /tmp/shared/ops_db.txt
-rw-rw-r-- 1 operator1 operators 0 Feb  4 16:11 /tmp/shared/ops_db.txt
```

- 7. Cree un archivo `ops_net.txt` en el directorio `/tmp/shared`. Registre la propiedad y los permisos. Cambie `umask` para el usuario `operator1`. Cree un archivo `ops_prod.txt`. Registre la propiedad y los permisos del archivo `ops_prod.txt`.

7.1. Cree un archivo `ops_net.txt` en el directorio `/tmp/shared`.

```
[operator1@servera ~]$ touch /tmp/shared/ops_net.txt
```

7.2. Enumere los permisos del archivo `ops_net.txt`.

```
[operator1@servera ~]$ ls -l /tmp/shared/ops_net.txt
-rw-rw-r-- 1 operator1 operators 5 Feb  0 15:43 /tmp/shared/ops_net.txt
```

7.3. Cambie el `umask` para el usuario `operator1` a 027. Confirme el cambio.

```
[operator1@servera ~]$ umask 027
[operator1@servera ~]$ umask
0027
```

- 7.4. Cree un archivo `ops_prod.txt` en el directorio `/tmp/shared/`. Verifique que los archivos creados recientemente tengan acceso de solo lectura para el grupo `operators` y sin acceso para otros usuarios.

```
[operator1@servera ~]$ touch /tmp/shared/ops_prod.txt
[operator1@servera ~]$ ls -l /tmp/shared/ops_prod.txt
-rw-r----- 1 operator1 operators 0 Feb  0 15:56 /tmp/shared/ops_prod.txt
```

- 8. Abra una nueva ventana de terminal e inicie sesión en `servera` como `operator1`.

```
[student@workstation ~]$ ssh operator1@servera
...output omitted...
[operator1@servera ~]$
```

- 9. Enumere el valor de `umask` para `operator1`.

```
[operator1@servera ~]$ umask
0002
```

- 10. Cambie el valor predeterminado de `umask` para el usuario `operator1`. El nuevo valor de `umask` prohíbe el acceso a los usuarios que no pertenezcan al grupo. Confirme que el `umask` presenta cambios.

10.1. Cambie el valor predeterminado de `umask` para el usuario `operator1` a 007.

```
[operator1@servera ~]$ echo "umask 007" >> ~/.bashrc
[operator1@servera ~]$ cat ~/.bashrc
# .bashrc

# Source global definitions
if [ -f /etc/bashrc ]; then
    . /etc/bashrc
fi
...output omitted...
umask 007
```

10.2. Cierre la sesión y vuelva a iniciar sesión como el usuario **operator1**. Confirme que el cambio sea permanente.

```
[operator1@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$ ssh operator1@servera
...output omitted...
[operator1@servera ~]$ umask
0007
```

- ▶ 11. En **servera**, cierre todas las shells de usuario **operator1** y **student**. Regrese al sistema **workstation** como el usuario **student**.



Advertencia

Si no sale de todas las shells **operator1**, el script de finalización fallará.

```
[operator1@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$
```

Finalizar

En la máquina **workstation**, cambie al directorio de inicio de usuario **student** y use el comando **lab** para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish perms-default
```

Esto concluye la sección.

► Trabajo de laboratorio

Control de acceso a los archivos

En este trabajo de laboratorio, establece permisos en los archivos y configura un directorio que los usuarios de un grupo particular pueden usar para compartir archivos en el sistema de archivos local.

Resultados

- Crear un directorio donde los usuarios puedan trabajar de forma conjunta en los archivos.
- Crear archivos que se asignan automáticamente a la propiedad del grupo.
- Crear archivos a los que no se pueda acceder fuera del grupo.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start perms-review
```

Instrucciones

1. Inicie sesión en `serverb` con el usuario `student`. Cambie al usuario `root` y use `redhat` como contraseña.
2. Cree un directorio `/home/techdocs`.
3. Cambie la propiedad del directorio `/home/techdocs` al grupo `techdocs`.
4. Verifique que los usuarios en el grupo `techdocs` no puedan crear archivos en el directorio `/home/techdocs`.
5. Establezca permisos en el directorio `/home/techdocs`. En el directorio `/home/techdocs`, configure `setgid` (2), permisos de lectura/escritura/ejecución (7) para el propietario/usuario y grupo, y ningún permiso (0) para otros usuarios.
6. Verifique que los permisos hayan sido establecidos correctamente.
El grupo `techdocs` ahora tiene permiso de escritura.
7. Confirme que los usuarios en el grupo `techdocs` ahora pueden crear y editar archivos en el directorio `/home/techdocs`. Los usuarios que no forman parte del grupo `techdocs` no pueden editar ni crear archivos en el directorio `/home/techdocs`. Los usuarios `tech1` y `tech2` están en el grupo `techdocs`. El usuario `database1` no está en ese grupo.
8. Modifique los scripts de inicio de sesión globales. Los usuarios normales deben tener una configuración de `umask` que permita al usuario y al grupo crear, escribir y ejecutar archivos y directorios, mientras evita que otros usuarios vean, modifiquen o ejecuten nuevos archivos y directorios.

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade perms-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish perms-review
```

Esto concluye la sección.

► Solución

Control de acceso a los archivos

En este trabajo de laboratorio, establece permisos en los archivos y configura un directorio que los usuarios de un grupo particular pueden usar para compartir archivos en el sistema de archivos local.

Resultados

- Crear un directorio donde los usuarios puedan trabajar de forma conjunta en los archivos.
- Crear archivos que se asignan automáticamente a la propiedad del grupo.
- Crear archivos a los que no se pueda acceder fuera del grupo.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start perms-review
```

Instrucciones

1. Inicie sesión en `serverb` con el usuario `student`. Cambie al usuario `root` y use `redhat` como contraseña.

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
[student@serverb ~]$ sudo -i
[sudo] password for student: student
[root@serverb ~]#
```

2. Cree un directorio `/home/techdocs`.
 - 2.1. Use el comando `mkdir` para crear un directorio `/home/techdocs`.

```
[root@serverb ~]# mkdir /home/techdocs
```

3. Cambie la propiedad del directorio `/home/techdocs` al grupo `techdocs`.
 - 3.1. Use el comando `chown` para cambiar la propiedad del grupo para el directorio `/home/techdocs` al grupo `techdocs`.

```
[root@serverb ~]# chown :techdocs /home/techdocs
```

4. Verifique que los usuarios en el grupo `techdocs` no puedan crear archivos en el directorio `/home/techdocs`.

- 4.1. Use el comando `su` para cambiar al usuario `tech1`.

```
[root@serverb ~]# su - tech1
[tech1@serverb ~]$
```

- 4.2. Cree un archivo `techdoc1.txt` en el directorio `/home/techdocs`. Este paso debería fallar.

Si bien el directorio `/home/techdocs` es propiedad del grupo `techdocs` y `tech1` es parte del grupo `techdocs`, no es posible crear un archivo en ese directorio. La razón es porque el grupo `techdocs` no tiene permiso de escritura.

```
[tech1@serverb ~]$ touch /home/techdocs/techdoc1.txt
touch: cannot touch '/home/techdocs/techdoc1.txt': Permission denied
```

- 4.3. Enumere los permisos del directorio.

```
[tech1@serverb ~]$ ls -ld /home/techdocs/
drwxr-xr-x. 2 root techdocs 6 Feb 5 16:05 /home/techdocs/
```

5. Establezca permisos en el directorio `/home/techdocs`. En el directorio `/home/techdocs`, configure `setgid` (2), permisos de lectura/escritura/ejecución (7) para el propietario/usuario y grupo, y ningún permiso (0) para otros usuarios.

- 5.1. Salga de la shell del usuario `tech1`.

```
[tech1@serverb ~]$ exit
logout
[root@serverb ~]#
```

- 5.2. Establezca el permiso del grupo para el directorio `/home/techdocs`. Configure `setgid`: permisos de lectura/escritura/ejecución para el propietario y el grupo, y ningún permiso para otros usuarios.

```
[root@serverb ~]# chmod 2770 /home/techdocs
```

6. Verifique que los permisos hayan sido establecidos correctamente.

```
[root@serverb ~]# ls -ld /home/techdocs
drwxrws---. 2 root techdocs 6 Feb 4 18:12 /home/techdocs/
```

El grupo `techdocs` ahora tiene permiso de escritura.

7. Confirme que los usuarios en el grupo `techdocs` ahora pueden crear y editar archivos en el directorio `/home/techdocs`. Los usuarios que no forman parte del grupo `techdocs` no pueden editar ni crear archivos en el directorio `/home/techdocs`. Los usuarios `tech1` y `tech2` están en el grupo `techdocs`. El usuario `database1` no está en ese grupo.

- 7.1. Cambie al usuario `tech1`. Cree un archivo `techdoc1.txt` en el directorio `/home/techdocs`. Salga de la shell del usuario `tech1`.

capítulo 4 | Control de acceso a los archivos

```
[root@serverb ~]# su - tech1
[tech1@serverb ~]$ touch /home/techdocs/techdoc1.txt
[tech1@serverb ~]$ ls -l /home/techdocs/techdoc1.txt
-rw-rw-r--. 1 tech1 techdocs 0 Feb  5 16:42 /home/techdocs/techdoc1.txt
[tech1@serverb ~]$ exit
logout
[root@serverb ~]#
```

- 7.2. Cambie al usuario **tech2**. Agregue algunos contenidos al archivo **/home/techdocs/techdoc1.txt**. Salga de la shell del usuario **tech2**.

```
[root@serverb ~]# su - tech2
[tech2@serverb ~]$ cd /home/techdocs
[tech2@serverb techdocs]$ echo "This is the first tech doc." > techdoc1.txt
[tech2@serverb techdocs]$ exit
logout
[root@serverb ~]#
```

- 7.3. Cambie al usuario **database1**. Agregue algunos contenidos al archivo **/home/techdocs/techdoc1.txt**. Recibe un mensaje **Permission Denied**. Verifique que **database1** no tenga acceso al archivo. Salga de la shell del usuario **database1**.

Ingrrese el siguiente comando largo echo en una sola línea:

```
[root@serverb ~]# su - database1
[database1@serverb ~]$ echo "This is the first tech doc." >> \
/home/techdocs/techdoc1.txt
-bash: /home/techdocs/techdoc1.txt: Permission denied
[database1@serverb ~]$ ls -l /home/techdocs/techdoc1.txt
ls: cannot access '/home/techdocs/techdoc1.txt': Permission denied
[database1@serverb ~]$ exit
logout
[root@serverb ~]#
```

8. Modifique los scripts de inicio de sesión globales. Los usuarios normales deben tener una configuración de umask que permita al usuario y al grupo crear, escribir y ejecutar archivos y directorios, mientras evita que otros usuarios vean, modifiquen o ejecuten nuevos archivos y directorios.

- 8.1. Determine el umask del usuario **student**. Cambie a la shell de inicio de sesión **student**. Salga de la shell cuando termine.

```
[root@serverb ~]# su - student
[student@serverb ~]$ umask
0002
[student@serverb ~]$ exit
logout
[root@serverb ~]#
```

- 8.2. Edite el archivo **/etc/profile** y agregue las siguientes propiedades del umask. El archivo **/etc/profile** ya contiene una definición de umask. Busque el archivo y actualice con los valores adecuados.

capítulo 4 | Control de acceso a los archivos

Establezca un umask de 007 para usuarios con un UID mayor que 199 y con un nombre de usuario y un nombre de grupo primario coincidentes. Establezca un umask de 022 para todos los demás.

En el siguiente ejemplo, se muestra el contenido agregado esperado en el archivo /etc/profile.

```
[root@serverb ~]# cat /etc/profile
...output omitted...
# Overrides default umask configuration
if [ $UID -gt 199 ] && [ "`id -gn`" = "`id -un`" ]; then
    umask 007
else
    umask 022
fi
...output omitted...
```

8.3. Con el usuario student, verifique que el umask global cambie a 007.

```
[root@serverb ~]# exit
logout
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@workstation ~]$ ssh student@serverb
...output omitted...
[student@serverb ~]$ umask
0007
```

8.4. Regrese al sistema workstation como el usuario student.

```
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@workstation ~]$
```

Evaluación

Con el usuario student en la máquina workstation, use el comando lab para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade perms-review
```

Finalizar

En la máquina workstation, cambie al directorio de inicio de usuario student y use el comando lab para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish perms-review
```

Esto concluye la sección.

Resumen

- El comando `chmod` cambia los permisos de archivo desde la línea de comandos.
- El comando `chmod` puede usar uno de dos métodos para representar permisos: simbólico u octal.
- El comando `chown` cambia la propiedad del archivo. El comando `chown` con la opción `-R` cambia recursivamente la propiedad de un árbol de directorios.
- El comando `umask` sin argumentos muestra el valor actual de umask de la shell. Todos los procesos del sistema tienen un umask. Los valores de umask predeterminados para Bash se definen en los archivos `/etc/profile` y `/etc/bashrc`.
- Los permisos especiales `suid`, `sgid` y `sticky` proporcionan funciones adicionales relacionadas con el acceso a los archivos.

capítulo 5

Administración de seguridad de SELinux

Meta

Proteger y administrar la seguridad del servidor con SELinux.

Objetivos

- Explicar cómo SELinux protege los recursos, cambiar el modo de SELinux actual de un sistema y definir el modo de SELinux predeterminado de un sistema.
- Administrar las reglas de política de SELinux que determinan el contexto predeterminado para archivos y directorios con el comando `semanage fcontext` y aplicar el contexto definido por la política de SELinux a archivos y directorios con el comando `restorecon`.
- Activar y desactivar las reglas de política de SELinux con el comando `setsebool`, administrar el valor persistente de los booleanos de SELinux con el comando `semanage boolean -l` y consultar las páginas `man` que terminan con `_selinux` para encontrar información útil acerca de los booleanos de SELinux.
- Usar las herramientas de análisis de registros de SELinux y visualizar información útil durante la solución de problemas de SELinux con el comando `sealert`.

Secciones

- Cambio del modo de cumplimiento (enforcement) de SELinux (y ejercicio guiado)
- Control de contextos de archivo de SELinux (y ejercicio guiado)
- Ajuste de la política de SELinux con booleanos (y ejercicio guiado)
- Investigación y resolución de problemas de SELinux (y ejercicio guiado)

Trabajo de laboratorio

Administración de seguridad de SELinux

Cambio del modo de cumplimiento (enforcement) de SELinux

Objetivos

Explicar cómo SELinux protege los recursos, cambiar el modo de SELinux actual de un sistema y definir el modo de SELinux predeterminado de un sistema.

Descripción de la arquitectura de SELinux

Security Enhanced Linux (SELinux) es una característica de seguridad fundamental de Linux. El acceso a los archivos, puertos y otros recursos se controla a un nivel granular. Los procesos tienen permitido el acceso solo a los recursos especificados por su política SELinux o parámetros booleanos.

Los permisos de archivos controlan el acceso a los archivos para un usuario o grupo específico. Sin embargo, los permisos de archivos no impiden que un usuario autorizado con acceso a archivos use un archivo para un propósito no deseado.

Por ejemplo, con acceso de escritura a un archivo, otros editores o programas aún pueden abrir y modificar un archivo de datos estructurado que está diseñado solo para escribir a un programa específico, lo que podría provocar daños o un problema de seguridad de datos. Los permisos de archivos no detienen dicho acceso no deseado porque no controlan cómo se usa un archivo, sino solo *quién* tiene permitido leer, escribir o ejecutar un archivo.

SELinux consta de políticas específicas de la aplicación que definen los desarrolladores de aplicaciones para declarar exactamente qué acciones y accesos están permitidos para cada ejecutable binario, archivo de configuración y archivo de datos usados por una aplicación. Esta política se conoce como *política dirigida*, ya que una política define las actividades de una aplicación. Las políticas declaran etiquetas predefinidas que se configuran en programas, archivos y puertos de red individuales.

Uso de SELinux

SELinux impone (enforce) un conjunto de reglas de acceso que definen explícitamente las acciones permitidas entre procesos y recursos. No se permite ninguna acción que no esté definida en una regla de acceso. Debido a que solo se permiten acciones definidas, las aplicaciones con un diseño de seguridad deficiente aún están protegidas del uso malintencionado. Las aplicaciones o los servicios con una política específica se ejecutan en un dominio *confinado*, mientras que una aplicación sin una política se ejecuta de forma *ilimitada* pero sin ninguna protección de SELinux. Las políticas específicas individuales se pueden deshabilitar para ayudar con el desarrollo y la depuración de políticas de seguridad y aplicaciones.

SELinux tiene los siguientes modos operativos:

- **Enforcing:** SELinux hace cumplir las políticas cargadas. Este modo es el predeterminado en Red Hat Enterprise Linux.
- **Permissive:** SELinux carga las políticas y está activo, pero en lugar de aplicar (enforcing) las reglas de control de acceso, registra las infracciones de acceso. Este modo es útil para probar y solucionar problemas de aplicaciones y reglas.
- **Disabled:** SELinux está desactivado. Las infracciones de SELinux no se rechazan ni se registran. Se desaconseja deshabilitar SELinux.



Importante

A partir de Red Hat Enterprise Linux 9, SELinux se puede deshabilitar por completo solo mediante el uso del parámetro de kernel `selinux=0` en el arranque. RHEL ya no soporta la configuración de la opción `SELINUX=disabled` en el archivo `/etc/selinux/config`.

A partir de RHEL 9, si se deshabilita SELinux en el archivo `/etc/selinux/config`, SELinux se inicia y ejecuta la aplicación activa (enforcing), pero sin cargar ninguna política. Debido a que las reglas de política definen acciones permitidas, si no se carga ninguna política, se rechazan todas las acciones. Este comportamiento es intencional y está diseñado para bloquear los intentos maliciosos de eludir la protección de SELinux.

Conceptos básicos de SELinux

El objetivo principal de SELinux es proteger los datos del usuario del uso inadecuado por parte de aplicaciones comprometidas o servicios de sistemas. La mayoría de los administradores de Linux están familiarizados con el modelo estándar de seguridad de permisos de archivos de usuarios, grupos y globales, que se conoce como *control de acceso discrecional (DAC)* porque los administradores definen los permisos de archivo según su necesidad. SELinux proporciona una capa adicional de seguridad basada en objetos, que se define en reglas granulares y se conoce como *control de acceso obligatorio (MAC)* porque las políticas de MAC se aplican a todos los usuarios y no se pueden omitir para usuarios específicos mediante ajustes de configuración discretionales.

Por ejemplo, el puerto de firewall abierto de un servidor web permite el acceso anónimo remoto a un cliente web. Sin embargo, un usuario malintencionado que accede a ese puerto puede intentar poner en peligro un sistema a través de una vulnerabilidad existente. Si una vulnerabilidad de ejemplo compromete los permisos para el usuario y el grupo apache, un usuario malintencionado puede acceder directamente al contenido raíz (root) del documento `/var/www/html`, a los directorios `/tmp` y `/var/tmp` del sistema, o a otros archivos y directorios accesibles.

Las políticas de SELinux son reglas de seguridad que definen cómo los procesos específicos acceden a archivos, directorios y puertos relevantes. Cada entidad de recursos, como un archivo, proceso, directorio o puerto, tiene una etiqueta denominada *contexto de SELinux*. La etiqueta de contexto coincide con una regla de política de SELinux definida para permitir que un proceso acceda al recurso etiquetado. De forma predeterminada, la política no permite ningún acceso a menos que una regla explícita otorgue acceso. Cuando no se define ninguna regla de permiso, no se permiten todos los accesos.

Las etiquetas de SELinux tienen campos `user`, `role`, `type` y `security_level`. La política específica, que está habilitada en RHEL de manera predeterminada, define reglas mediante el uso del contexto `type`. Por lo general, los nombres de contexto de tipo finalizan en `_t`.

<i>SELinux User</i>	<i>Role</i>	<i>Type</i>	<i>Level</i>	<i>File</i>
<code>unconfined_u:object_r:httpd_sys_content_t:s0</code>		<code>/var/www/html/file2</code>		

Figura 5.1: Contexto de archivo de SELinux

Conceptos de reglas de acceso a políticas

Por ejemplo, un proceso de servidor web se etiqueta con el contexto de tipo `httpd_t`. Los archivos y directorios del servidor web en el directorio `/var/www/html/` y otras ubicaciones

se etiquetan con el contexto de tipo `httpd_sys_content_t`. Los archivos temporales en los directorios `/tmp` y `/var/tmp` tienen los contextos de tipo `tmp_t` como etiqueta. Los puertos del servidor web tienen el contexto de tipo `http_port_t` como etiqueta.

Un proceso de servidor web Apache se ejecuta con el contexto de tipo `httpd_t`. Una regla de política permite que el servidor Apache acceda a archivos y directorios con la etiqueta de contexto de tipo `httpd_sys_content_t`. De manera predeterminada, los archivos en el directorio `/var/www/html` tienen el contexto de tipo `httpd_sys_content_t`. De manera predeterminada, una política de servidor web no tiene reglas `allow` para usar archivos con la etiqueta `tmp_t`, como en los directorios `/tmp` y `/var/tmp`, lo que impide el acceso. Con SELinux habilitado, un usuario malintencionado que usa un proceso Apache comprometido aún no podría acceder al directorio `/tmp`.

Un proceso de servidor web MariaDB se ejecuta con el contexto de tipo `mysqld_t`. De manera predeterminada, los archivos en el directorio `/data/mysql` tienen el contexto de tipo `mysqld_db_t`. Un servidor MariaDB puede acceder a los archivos etiquetados `mysqld_db_t`, pero no tiene reglas para permitir el acceso a los archivos para otros servicios, como los archivos etiquetados `httpd_sys_content_t`.

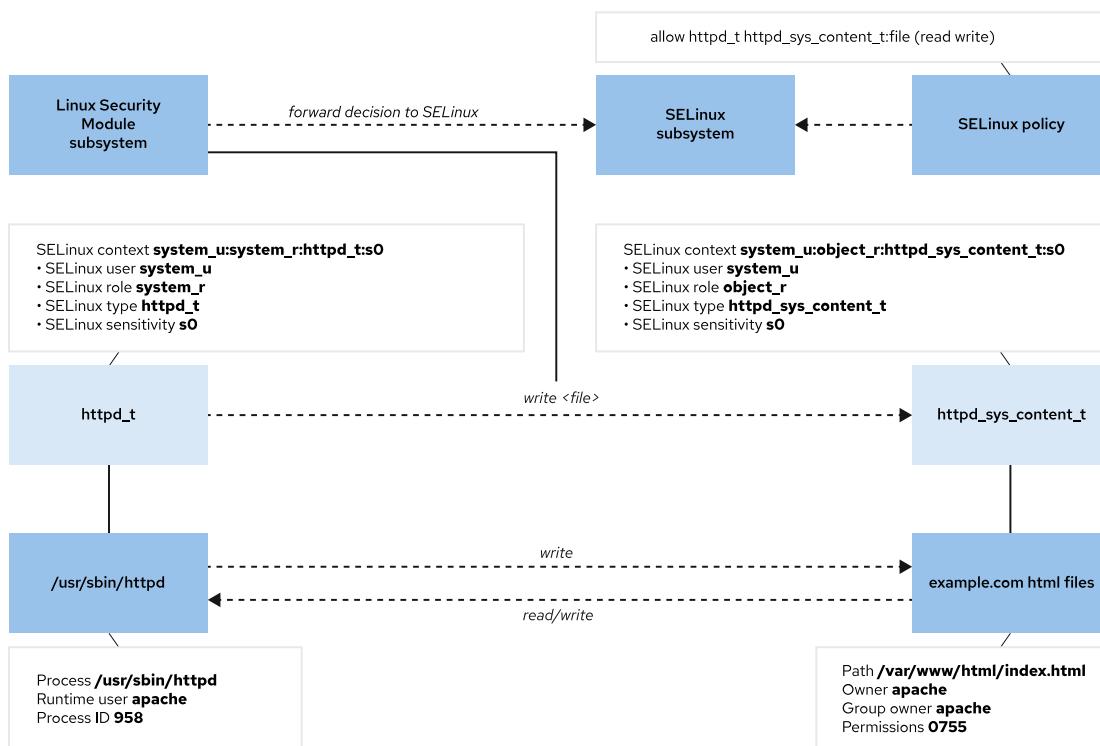


Figura 5.2: Flujo de toma de decisiones de SELinux

Muchos comandos que enumeran recursos usan la opción `-Z` para administrar contextos de SELinux. Por ejemplo, los comandos `ps`, `ls`, `cp` y `mkdir` usan la opción `-Z`.

```
[root@host ~]# ps axZ
LABEL PID TTY STAT TIME COMMAND
system_u:system_r:kernel_t:s0 2 ? S 0:00 [kthreadd]
system_u:system_r:kernel_t:s0 3 ? I< 0:00 [rcu_gp]
system_u:system_r:kernel_t:s0 4 ? I< 0:00 [rcu_par_gp]
...output omitted...
[root@host ~]# systemctl start httpd
[root@host ~]# ps -ZC httpd
```

LABEL	PID	TTY	TIME	CMD
system_u:system_r:httpd_t:s0	1550	?	00:00:00	httpd
system_u:system_r:httpd_t:s0	1551	?	00:00:00	httpd
system_u:system_r:httpd_t:s0	1552	?	00:00:00	httpd
system_u:system_r:httpd_t:s0	1553	?	00:00:00	httpd
system_u:system_r:httpd_t:s0	1554	?	00:00:00	httpd
[root@host ~]# ls -Z /var/www				
system_u:object_r:httpd_sys_script_exec_t:s0		cgi-bin		
system_u:object_r:httpd_sys_content_t:s0		html		

Cambio del modo de SELinux

Use el comando `getenforce` para ver el modo actual de SELinux. Use el comando `setenforce` para cambiar el modo actual de SELinux.

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

De manera alternativa, defina el modo SELinux en el momento del arranque con un parámetro del kernel. Pase el parámetro del kernel `enforcing=0` para arrancar el sistema en modo `permissive` o pase `enforcing=1` para arrancar en modo `enforcing`. Deshabilite SELinux pasando el parámetro del kernel `selinux=0` o pase `selinux=1` para habilitar SELinux.

Red Hat recomienda reiniciar el servidor cuando cambie el modo de SELinux de `Permissive` a `Enforcing`. Este reinicio garantiza que los servicios iniciados en modo `permissive` estén limitados en el siguiente arranque.

Configuración del modo predeterminado de SELinux

Para configurar SELinux de manera persistente, use el archivo `/etc/selinux/config`. En el siguiente ejemplo predeterminado, la configuración establece SELinux en el modo `enforcing`. Los comentarios enumeran otros valores válidos, como los modos `permissive` y `disabled`.

```
# 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.
...output omitted...
#
# NOTE: In earlier Fedora kernel builds, SELINUX=disabled would also
# fully disable SELinux during boot. If you need a system with SELinux
# fully disabled instead of SELinux running with no policy loaded, you
# need to pass selinux=0 to the kernel command line. You can use grubby
# to persistently set the bootloader to boot with selinux=0:
#
```

```
#      grubby --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
#      grubby --update-kernel ALL --remove-args selinux
#
SELINUX=enforcing
# SELINUXTYPE= can take one of these three values:
#      targeted - Targeted processes are protected,
#      minimum - Modification of targeted policy. Only selected processes are
protected.
#      mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

El sistema lee este archivo en el momento del arranque y configura SELinux en consecuencia. Los argumentos del kernel `selinux=0|1` y `enforcing=0|1` anulan esta configuración.



Referencias

Páginas del manual: `getenforce(8)`, `setenforce(8)` y `selinux_config(5)`

► Ejercicio Guiado

Cambio del modo de cumplimiento (enforcement) de SELinux

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

Resultados

- Ver y configurar el modo de SELinux actual.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start selinux-opsmode
```

Instrucciones

- 1. En la máquina `workstation`, use el comando `ssh` para iniciar sesión en la máquina `servera` como el usuario `student` y, luego, cambie al usuario `root`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

- 2. Cambie el modo predeterminado de SELinux a permissive.

- 2.1. Use el comando `getenforce` para verificar el modo actual de SELinux en la máquina `servera`.

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

- 2.2. Use el comando `vim /etc/selinux/config` para editar el archivo de configuración. Cambie el parámetro SELINUX del modo `enforcing` a `permissive`.

```
[root@servera ~]# vim /etc/selinux/config
```

- 2.3. Use el comando `grep` para confirmar que el parámetro SELINUX se muestra el modo `permissive`.

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

- 2.4. Use el comando `getenforce` para confirmar que el parámetro SELINUX se muestra en el modo `enforcing`.

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

- 2.5. Use el comando `setenforce` para cambiar el modo SELINUX al modo `permissive` y verifique el cambio.

```
[root@servera ~]# setenforce 0
[root@servera ~]# getenforce
Permissive
```

- 3. Cambie el modo predeterminado de SELinux al modo `enforcing` en el archivo de configuración.
- 3.1. Use el comando `vim /etc/selinux/config` para editar el archivo de configuración. Cambie el parámetro SELINUX del modo `permissive` a `enforcing`.

```
[root@servera ~]# vim /etc/selinux/config
```

- 3.2. Use el comando `grep` para confirmar que el parámetro SELINUX define el modo `enforcing` en inicio

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

- 4. Defina el modo SELinux en `enforcing` en la línea de comandos. Reinicie la máquina `servera` y verifique el modo SELinux.
- 4.1. Use el comando `setenforce` para definir el modo actual de SELinux en el modo `enforcing`. Use el comando `getenforce` para confirmar que SELinux está en el modo `enforcing`.

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

- 4.2. Reinicie la máquina `servera` para implementar la configuración persistente.

```
[root@servera ~]# systemctl reboot
Connection to servera closed by remote host.
Connection to servera closed.
[student@workstation ~]$
```

4.3. Inicie sesión en la máquina servera y verifique el modo SELinux.

```
[student@workstation ~]$ ssh student@servera  
...output omitted...  
[student@servera ~]$ sudo -i  
[sudo] password for student: student  
[root@servera ~]# getenforce  
Enforcing
```

▶ 5. Regrese a la máquina workstation como el usuario student.

```
[root@servera ~]# exit  
logout  
[student@servera ~]$ exit  
logout  
Connection to servera closed.  
[student@workstation ~]$
```

Finalizar

En la máquina **workstation**, cambie al directorio de inicio de usuario **student** y use el comando **lab** para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish selinux-opsmode
```

Esto concluye la sección.

Control de contextos de archivo de SELinux

Objetivos

Administrar las reglas de política de SELinux que determinan el contexto predeterminado para archivos y directorios con el comando `semanage fcontext` y aplicar el contexto definido por la política de SELinux a archivos y directorios con el comando `restorecon`.

Contexto inicial de SELinux

Todos los recursos, como procesos, archivos y puertos, se etiquetan con un contexto de SELinux. SELinux mantiene una base de datos basada en archivos de políticas de etiquetado de archivos en el directorio `/etc/selinux/targeted-contexts/files/`. Los archivos nuevos obtienen una etiqueta predeterminada cuando su nombre de archivo coincide con una política de etiquetado existente.

Cuando el nombre de un archivo nuevo no coincide con una política de etiquetado existente, el archivo hereda la misma etiqueta que el directorio principal. Con la herencia de etiquetado, todos los archivos siempre se etiquetan cuando se crean, independientemente de si existe una política explícita para un archivo.

Cuando se crean archivos en ubicaciones predeterminadas que tienen una política de etiquetado existente, o cuando existe una política para una ubicación personalizada, los archivos nuevos se etiquetan con un contexto SELinux correcto. Sin embargo, si se crea un archivo en una ubicación inesperada sin una política de etiquetado existente, es posible que la etiqueta heredada no sea correcta para el propósito previsto del nuevo archivo.

Además, copiar un archivo en una nueva ubicación puede hacer que el contexto de SELinux de ese archivo cambie, con el nuevo contexto determinado por la política de etiquetado de la nueva ubicación o por la herencia del directorio principal si no existe una política. El contexto de SELinux de un archivo se puede conservar durante una copia para conservar la etiqueta de contexto que se determinó para la ubicación original del archivo. Por ejemplo, el comando `cp -p` conserva todos los atributos del archivo cuando sea posible y el comando `cp -c` conserva solo los contextos de SELinux durante una copia.



nota

Copiar un archivo crea siempre un nuevo inodo de archivo, y los atributos de ese inodo, incluido el contexto de SELinux, deben establecerse inicialmente, como se analizó anteriormente.

Sin embargo, mover un archivo generalmente no crea un nuevo inodo si el movimiento ocurre dentro del mismo sistema de archivos, sino que mueve el nombre de archivo del inodo existente a una nueva ubicación. Debido a que los atributos del inodo existente no necesitan inicializarse, un archivo que se mueve con `mv` conserva su contexto de SELinux a menos que usted establezca un nuevo contexto en el archivo con la opción `-Z`.

Después de copiar o mover un archivo, verifique que tenga el contexto de SELinux adecuado y configúrelo correctamente si es necesario.

El siguiente ejemplo demuestra cómo funciona este proceso.

Cree dos archivos vacíos en el directorio /tmp. Ambos archivos reciben el tipo de contexto user_tmp_t.

Mueva el primer archivo y copie el segundo archivo al directorio /var/www/html.

- El archivo movido conserva el contexto de archivo que se etiquetó desde el directorio /tmp original.
- El archivo copiado tiene un nuevo inodo y hereda el contexto de SELinux del directorio de destino /var/www/html.

El comando ls -Z muestra el contexto de SELinux de un archivo. Observe la etiqueta de los archivos creados en el directorio /tmp.

```
[root@host ~]# touch /tmp/file1 /tmp/file2
[root@host ~]# ls -Z /tmp/file*
unconfined_u:object_r:user_tmp_t:s0 /tmp/file1
unconfined_u:object_r:user_tmp_t:s0 /tmp/file2
```

El comando ls -Zd muestra el contexto de SELinux del directorio especificado. Observe la etiqueta en el directorio /var/www/html y los archivos que contiene.

```
[root@host ~]# ls -Zd /var/www/html/
system_u:object_r:httpd_sys_content_t:s0 /var/www/html/
[root@host ~]# ls -Z /var/www/html/index.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/index.html
```

Mueva un archivo del directorio /tmp al directorio /var/www/html. Copie el otro archivo al mismo directorio. Observe la etiqueta resultante en cada archivo.

```
[root@host ~]# mv /tmp/file1 /var/www/html/
[root@host ~]# cp /tmp/file2 /var/www/html/
[root@host ~]# ls -Z /var/www/html/file*
unconfined_u:object_r:user_tmp_t:s0 /var/www/html/file1
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/file2
```

El archivo movido conservó su etiqueta original y el archivo copiado heredó la etiqueta del directorio de destino. Aunque no es importante para este análisis, unconfined_u es el usuario de SELinux, object_r es el rol de SELinux y s0 es el nivel de sensibilidad (más bajo posible). Las configuraciones y características avanzadas de SELinux usan estos valores.

Cambio del contexto de SELinux

Puede cambiar los contextos de SELinux en los archivos con los comandos semanage fcontext, restorecon y chcon.

El método recomendado para definir el contexto para un archivo es crear una política de contexto de archivo con el comando semanage fcontext y, luego, aplicar el contexto especificado en la política al archivo con el comando restorecon. Este método garantiza que pueda volver a etiquetar fácilmente el archivo en su contexto correcto con el comando restorecon siempre que sea necesario. La ventaja de este método es que no necesita recordar cuál se supone que es el contexto y puede corregir fácilmente el contexto en un conjunto de archivos.

El comando `chcon` define el contexto de SELinux directamente en los archivos, pero sin hacer referencia a la política de SELinux del sistema. Si bien `chcon` es útil para probar y depurar, la configuración manual de contextos con este método es temporal. Los contextos de archivos que se establecen manualmente sobreviven a un reinicio, pero pueden reemplazarse si ejecuta `restorecon` para volver a etiquetar el contenido del sistema de archivos.



Importante

Cuando se produce una *nueva etiqueta* del sistema SELinux, todos los archivos en un sistema se etiquetan con sus valores predeterminados de política. Cuando usa `restorecon` en un archivo, cualquier contexto que configure manualmente en el archivo se reemplaza si no coincide con las reglas de la política de SELinux.

El siguiente ejemplo crea un directorio con un contexto de SELinux `default_t`, que heredó del directorio principal `/`.

```
[root@host ~]# mkdir /virtual
[root@host ~]# ls -Zd /virtual
unconfined_u:object_r:default_t:s0 /virtual
```

El comando `chcon` define el contexto de archivo del directorio `/virtual` en el tipo `httpd_sys_content_t`.

```
[root@host ~]# chcon -t httpd_sys_content_t /virtual
[root@host ~]# ls -Zd /virtual
unconfined_u:object_r:httpd_sys_content_t:s0 /virtual
```

La ejecución del comando `restorecon` restablece el contexto al valor predeterminado de `default_t`. Observe el mensaje `Relabeled`.

```
[root@host ~]# restorecon -v /virtual
Relabeled '/virtual' from unconfined_u:object_r:httpd_sys_content_t:s0 to
unconfined_u:object_r:default_t:s0
[root@host ~]# ls -Zd /virtual
unconfined_u:object_r:default_t:s0 /virtual
```

Definición de las políticas de contextos de archivos predeterminados de SELinux

El comando `semanage fcontext` muestra o modifica las políticas que determina los contextos de archivos predeterminados. Puede enumerar todas las reglas de políticas de contexto de archivos ejecutando el comando `semanage fcontext -l`. Estas reglas usan la sintaxis de expresiones regulares para especificar los nombres de archivo y las rutas de acceso.

Al visualizar políticas, la expresión regular extendida más común es `(/.*)?`, que generalmente se anexa al nombre de un directorio. Esta notación se denomina humorísticamente *pirata*, porque tiene el aspecto de una cara con un parche en el ojo y una mano en forma de gancho al lado.

Esta sintaxis se describe como "un conjunto de caracteres que comienza con una barra y va seguido de cualquier número de caracteres, donde el conjunto puede existir o no". Dicho de manera más simple, esta sintaxis coincide con el directorio en sí, incluso cuando está vacío, pero también coincide con casi cualquier nombre de archivo que se crea dentro de ese directorio.

Por ejemplo, la siguiente regla especifica que el directorio `/var/www/cgi-bin` y cualquier archivo en él o en sus subdirectorios (y sus subdirectorios, etc.) deben tener el contexto de SELinux `system_u:object_r:httpd_sys_script_exec_t:s0`, salvo que una regla más específica lo anule.

```
/var/www/cgi-bin(/.*)? all files system_u:object_r:httpd_sys_script_exec_t:s0
```

Operaciones básicas de contexto de archivo

La siguiente tabla es una referencia para las opciones del comando `semanage fcontext` para agregar, eliminar o enumerar políticas de contextos de archivos de SELinux.

Comandos de semanage fcontext

opción	descripción
<code>-a, --add</code>	Agregar un registro del tipo de objeto especificado
<code>-d, --delete</code>	Eliminar un registro del tipo de objeto especificado
<code>-l, --list</code>	Mostrar registros del tipo de objeto especificado

Para administrar contextos de SELinux, instale los paquetes `policycoreutils` y `policycoreutils-python-utils`, que contienen los comandos `restorecon` y `semanage`.

Para restablecer todos los archivos en un directorio al contexto de política predeterminado, primero use el comando `semanage fcontext -l` para localizar y verificar que la política correcta existe con el contexto de archivo deseado. A continuación, use el comando `restorecon` en el nombre del directorio con comodines para restablecer todos los archivos de manera recursiva. En el siguiente ejemplo, vea los contextos de archivos antes y después de usar los comandos `semanage` y `restorecon`.

Primero, verifique el contexto de SELinux para los archivos:

```
[root@host ~]# ls -Z /var/www/html/file*
unconfined_u:object_r:user_tmp_t:s0 /var/www/html/file1
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/file2
```

A continuación, use el comando `semanage fcontext -l` para enumerar los contextos de archivos SELinux predeterminados:

```
[root@host ~]# semanage fcontext -l
...output omitted...
/var/www(/.*)?      all files      system_u:object_r:httpd_sys_content_t:s0
...output omitted...
```

La salida del comando `semanage` indica que todos los archivos y subdirectorios en el directorio `/var/www/` tendrán el contexto `httpd_sys_content_t` de manera predeterminada. La ejecución del comando `restorecon` en la carpeta con comodines restaura el contexto predeterminado en todos los archivos y subdirectorios.

```
[root@host ~]# restorecon -Rv /var/www/
Relabeled /var/www/html/file1 from unconfined_u:object_r:user_tmp_t:s0 to
unconfined_u:object_r:httpd_sys_content_t:s0
[root@host ~]# ls -Z /var/www/html/file*
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/file1
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/file2
```

El siguiente ejemplo usa el comando semanage para agregar una política de contexto para un directorio nuevo. Primero, cree el directorio `/virtual` con un archivo `index.html` en él. Vea el contexto de SELinux para el archivo y el directorio.

```
[root@host ~]# mkdir /virtual
[root@host ~]# touch /virtual/index.html
[root@host ~]# ls -Zd /virtual/
unconfined_u:object_r:default_t:s0 /virtual
[root@host ~]# ls -Z /virtual/
unconfined_u:object_r:default_t:s0 index.html
```

A continuación, use el comando `semanage fcontext` para agregar una política de contexto de archivo SELinux para el directorio.

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

Use el comando `restorecon` en el directorio con comodines para definir el contexto predeterminado en el directorio y todos los archivos dentro de él.

```
[root@host ~]# restorecon -RFvv /virtual
Relabeled /virtual from unconfined_u:object_r:default_t:s0 to
system_u:object_r:httpd_sys_content_t:s0
Relabeled /virtual/index.html from unconfined_u:object_r:default_t:s0 to
system_u:object_r:httpd_sys_content_t:s0
[root@host ~]# ls -Zd /virtual/
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 /virtual/
[root@host ~]# ls -Z /virtual/
-rw-r--r--. root root system_u:object_r:httpd_sys_content_t:s0 index.html
```

Use el comando `semanage fcontext -l -C` para ver las personalizaciones locales de la política predeterminada.

```
[root@host ~]# semanage fcontext -l -C
SELinux fcontext      type          Context
/virtual(/.*)?        all files    system_u:object_r:httpd_sys_content_t:s0
```



Referencias

Páginas del manual: `chcon(1)`, `restorecon(8)`, `semanage(8)` y `semanage-fcontext(8)`

► Ejercicio Guiado

Control de contextos de archivo de SELinux

En este trabajo de laboratorio, realiza un cambio persistente en el contexto de SELinux de un directorio y su contenido.

Resultados

- Configure el servidor HTTP Apache para publicar contenido web desde una raíz (root) de documento no estándar.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start selinux-filecontexts
```

Instrucciones

- 1. Inicie sesión en `servera` como el usuario `student` y cambie al usuario `root`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

- 2. Configure Apache para usar un directorio de documento en una ubicación no estándar.

- 2.1. Cree el directorio `/custom`.

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

- 2.2. Cree el archivo `index.html` en el directorio `/custom`. El archivo `index.html` debe contener el texto `This is SERVERA..`

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

- 2.3. Configure Apache para que use la nueva ubicación del directorio. Edite el archivo de configuración de Apache `/etc/httpd/conf/httpd.conf` y reemplace las dos apariciones del directorio `/var/www/html` con el directorio `/custom`. Puede usar

el comando `vim /etc/httpd/conf/httpd.conf` para hacerlo. En el siguiente ejemplo, se muestra el contenido esperado del archivo `/etc/httpd/conf/httpd.conf`.

```
[root@servera ~]# cat /etc/httpd/conf/httpd.conf
...output omitted...
DocumentRoot "/custom"
...output omitted...
<Directory "/custom">
...output omitted...
```

- 3. Inicie y habilite el servicio web Apache y confirme que el servicio se está ejecutando.

- 3.1. Inicie y habilite el servicio web Apache con el comando `systemctl`.

```
[root@servera ~]# systemctl enable --now httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/
lib/systemd/system/httpd.service.
```

- 3.2. Verifique que el servicio se esté ejecutando.

```
[root@servera ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor
  preset: disabled)
    Active: active (running) since Wed 2022-04-06 05:21:19 EDT; 22s ago
      Docs: man:httpd.service(8)
     Main PID: 1676 (httpd)
...output omitted...
Apr 06 05:21:19 servera.lab.example.com systemd[1]: Starting The Apache HTTP
Server...
Apr 06 05:21:19 servera.lab.example.com systemd[1]: Started The Apache HTTP
Server.
Apr 06 05:21:19 servera.lab.example.com httpd[1676]: Server configured, listening
on: port 80
```

- 4. Abra un navegador web en `workstation` e intente ver la página web `http://servera/index.html`. Recibe un mensaje de error indicando que no tiene permiso para acceder al archivo.
- 5. Para permitir el acceso al archivo `index.html` en `servera`, debe configurar el contexto de SELinux. Defina una regla de contextos de archivos de SELinux que defina el tipo de contexto en `httpd_sys_content_t` para el directorio `/custom` y todos los archivos en él.

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

- 6. Corrija los contextos de archivos en el directorio `/custom`.

```
[root@servera ~]# restorecon -Rv /custom
Relabeled /custom from unconfined_u:object_r:default_t:s0 to
unconfined_u:object_r:httpd_sys_content_t:s0
Relabeled /custom/index.html from unconfined_u:object_r:default_t:s0 to
unconfined_u:object_r:httpd_sys_content_t:s0
```

- ▶ 7. Intente ver `http://servera/index.html` nuevamente en el navegador web en la máquina `workstation`. Deberá ver el mensaje `This is SERVERA..`
- ▶ 8. Regrese a la máquina `workstation` como el usuario `student`.

```
[root@servera ~]# exit
logout
[student@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish selinux-filecontexts
```

Esto concluye la sección.

Ajuste de la política de SELinux con booleanos

Objetivos

Activar y desactivar las reglas de política de SELinux con el comando `setsebool`, administrar el valor persistente de los booleanos de SELinux con el comando `semanage boolean -l` y consultar las páginas `man` que terminan con `_selinux` para encontrar información útil acerca de los booleanos de SELinux.

Booleanos de SELinux

Un desarrollador de aplicaciones o servicios escribe una política específica de SELinux para definir el comportamiento permitido de la aplicación de destino. Un desarrollador puede incluir un comportamiento de aplicación opcional en la política de SELinux que se puede habilitar cuando el comportamiento está permitido en un sistema específico. Los booleanos de SELinux habilitan o deshabilitan el comportamiento opcional de la política de SELinux. Con los booleanos, puede ajustar selectivamente el comportamiento de una aplicación.

Estos comportamientos opcionales son específicos de la aplicación y deben detectarse y seleccionarse para cada aplicación de destino. Los booleanos específicos del servicio están documentados en la página del manual de SELinux de ese servicio. Por ejemplo, el servicio `httpd` del servidor web tiene su página de manual `httpd(8)` y una página de manual `httpd_selinux(8)` para documentar su política de SELinux, incluidos los tipos de procesos soportados, los contextos de archivos y los comportamientos booleanos disponibles. Las páginas del manual de SELinux se proporcionan en el paquete `selinux-policy-doc`.

Use el comando `getsebool` para enumerar los booleanos disponibles para las políticas objetivo en este sistema y el estado booleano actual. Use el comando `setsebool` para habilitar o deshabilitar el estado de ejecución de estos comportamientos. La opción del comando `setsebool -P` hace que la configuración sea persistente al escribir en el archivo de políticas. Solo los usuarios con privilegios pueden definir booleanos de SELinux.

```
[root@host ~]# getsebool -a
abrt_anon_write --> off
abrt_handle_event --> off
abrt_upload_watch_anon_write --> on
...output omitted...
```

Ejemplo de booleano de política httpd

La política de servicio `httpd` incluye el booleano `httpd_enable_homedirs` que permite compartir directorios de inicio con `httpd`. Por lo general, el directorio de inicio local de un usuario solo es accesible para el usuario cuando está conectado al sistema local. De manera alternativa, los directorios de inicio se comparten y se accede a ellos mediante un protocolo de uso compartido de archivos remoto, como NFS. En ambas situaciones, los directorios de inicio no se comparten mediante el uso de `https`, de manera predeterminada, y no están disponibles para el usuario a través de un navegador.

```
[root@host ~]# getsebool httpd_enable_homedirs
httpd_enable_homedirs --> off
```

Puede habilitar el uso compartido y permitir que los usuarios accedan a sus directorios de inicio con un navegador. Cuando está habilitado, el servicio `httpd` comparte directorios de inicio que están etiquetados con el contexto de archivo `user_home_dir_t`. Los usuarios pueden acceder y administrar sus archivos de directorio de inicio desde un navegador.

Administración del booleano de la política

La configuración de booleanos de SELinux con el comando `setsebool` sin la opción `-P` es temporal, y la configuración volverá a los valores persistentes después del reinicio. Vea información adicional con el comando `semanage boolean -l`, que enumera los booleanos de los archivos de política, incluido si un booleano es persistente, los valores predeterminados y actuales y una breve descripción.

```
[root@host ~]# semanage boolean -l | grep httpd_enable_homedirs
httpd_enable_homedirs          (off , off)  Allow httpd to enable homedirs
[root@host ~]# setsebool httpd_enable_homedirs on
[root@host ~]# semanage boolean -l | grep httpd_enable_homedirs
httpd_enable_homedirs          (on , off)  Allow httpd to enable homedirs
[root@host ~]# getsebool httpd_enable_homedirs
httpd_enable_homedirs --> on
```

Para enumerar solo los booleanos con una configuración actual diferente de la configuración predeterminada en el arranque, use el comando `semanage boolean -l -C`. Este ejemplo tiene el mismo resultado que el ejemplo anterior, sin requerir el filtrado `grep`.

```
[root@host ~]# semanage boolean -l -C
SELinux boolean           State  Default Description
httpd_enable_homedirs     (on , off)  Allow httpd to enable homedirs
```

En el ejemplo anterior se definió temporalmente el valor actual para el booleano `httpd_enable_homedirs` en `on`, hasta que el sistema se reinicia. Para cambiar la configuración predeterminada, use el comando `setsebool -P` para hacer que la configuración sea persistente. En el siguiente ejemplo se define un valor persistente y, luego, se visualiza la información booleana del archivo de política.

```
[root@host ~]# setsebool -P httpd_enable_homedirs on
[root@host ~]# semanage boolean -l | grep httpd_enable_homedirs
httpd_enable_homedirs     (on , on)  Allow httpd to enable homedirs
```

Use el comando `semanage boolean -l -C` de nuevo. El booleano se muestra a pesar de que la configuración actual y predeterminada es la misma. Sin embargo, la opción `-C` coincide cuando la configuración actual es diferente de la configuración predeterminada del último arranque. Para este ejemplo de `httpd_enable_homedirs`, la configuración de arranque predeterminada original era `off`.

```
[root@host ~]# semanage boolean -l -C
SELinux boolean          State  Default Description
httpd_enable_homedirs    (on   ,   on)  Allow httpd to enable homedirs
```



Referencias

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

► Ejercicio Guiado

Ajuste de la política de SELinux con booleanos

En este ejercicio, configurará Apache para publicar contenido web desde los directorios de inicio de los usuarios.

Resultados

- Configure el servicio web Apache para publicar contenido web desde el directorio de inicio del usuario.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start selinux-booleans
```

Instrucciones

- 1. En la máquina `workstation`, use el comando `ssh` para iniciar sesión en la máquina `servera` como el usuario `student` y, luego, cambie al usuario `root`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

- 2. Edite el archivo de configuración `/etc/httpd/conf.d/userdir.conf` para habilitar la función Apache para que los usuarios puedan publicar contenido web desde sus directorios de inicio. Comente la línea en la sección `IfModule` que define la variable `UserDir` en el valor `disabled` y quite el comentario de la línea que define la variable `UserDir` en el valor `public_html`.

```
[root@servera ~]# vim /etc/httpd/conf.d/userdir.conf
<IfModule mod_userdir.c>
...output omitted...
# UserDir disabled

...output omitted...
UserDir public_html
```

```
...output omitted...
</IfModule>
```

- 3. Inicie y habilite el servicio web Apache.

```
[root@servera ~]# systemctl enable --now httpd
```

- 4. Abra otra ventana de terminal y use el comando ssh para iniciar sesión en la máquina servera con el usuario student. Cree el archivo de contenido web index.html en el directorio ~/public_html.

- 4.1. En otra ventana de terminal, use el comando ssh para iniciar sesión en la máquina servera con el usuario student.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

- 4.2. Use el comando mkdir para crear el directorio ~/public_html.

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

- 4.3. Cree el archivo index.html con el siguiente contenido:

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

- 4.4. Para que el servicio web Apache proporcione el contenido del directorio /home/student/public_html, debe tener permiso para compartir archivos y subdirectorios en el directorio /home/student. Cuando creó el directorio /home/student/public_html, se configuró automáticamente con permisos que permiten a cualquier persona con permiso de directorio de inicio acceder a su contenido.

Cambie los permisos del directorio /home/student para permitir que el servicio web Apache acceda al subdirectorio public_html.

```
[student@servera ~]$ chmod 711 ~
[student@servera ~]$ ls -ld ~
drwx--x--x. 16 student student 4096 Nov  3 09:28 /home/student
```

- 5. Abra un navegador web en la máquina workstation e ingrese la dirección http://servera/~student/index.html. Un mensaje de error indica que no tiene permiso para acceder al archivo.
- 6. Cambie al otro terminal y use el comando getsebool para ver si algún booleano restringe el acceso a los directorios para el servicio httpd.

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

- 7. Use el comando `setsebool` para habilitar el acceso persistente al directorio de inicio para el servicio `httpd`.

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

- 8. Verifique que ahora pueda ver el mensaje `This is student content on SERVERA.` en el navegador web después de ingresar la dirección `http://servera/~student/index.html`.
- 9. Regrese a la máquina `workstation` como el usuario `student`.

```
[root@servera ~]# exit  
logout  
[student@servera ~]$ exit  
logout  
Connection to servera closed.  
[student@workstation ~]$
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish selinux-booleans
```

Esto concluye la sección.

Investigación y resolución de problemas de SELinux

Objetivos

Usar las herramientas de análisis de registros de SELinux y visualizar información útil durante la solución de problemas de SELinux con el comando `sealert`.

Solución de problemas de SELinux

Cuando las aplicaciones inesperadamente no funcionan debido a denegaciones de acceso a SELinux, existen métodos y herramientas disponibles para resolver estos problemas. Es útil comenzar por comprender algunos conceptos y comportamientos fundamentales cuando SELinux está habilitado.

- SELinux consta de políticas específicas que definen explícitamente las acciones permitidas.
- Una entrada de política define un proceso etiquetado y un recurso etiquetado que interactuará.
- La política establece el tipo de proceso y el contexto de archivo o puerto mediante el uso de etiquetas.
- La entrada de política define un tipo de proceso, una etiqueta de recurso y la acción explícita para permitir.
- Una acción puede ser una llamada al sistema, una función del kernel u otra rutina de programación específica.
- Si no se crea una entrada para una relación específica entre el proceso, el recurso y la acción, se rechaza la acción.
- Cuando se rechaza una acción, el intento se registra con información útil de contexto.

Red Hat Enterprise Linux proporciona una política de SELinux específica y estable para casi todos los servicios de la distribución. Por lo tanto, es inusual tener problemas de acceso de SELinux con los servicios comunes de RHEL cuando están configurados correctamente. Los problemas de acceso a SELinux ocurren cuando los servicios se implementan incorrectamente o cuando las nuevas aplicaciones tienen políticas incompletas. Tenga en cuenta estos conceptos de solución de problemas antes de realizar cambios generales en la configuración de SELinux.

- La mayoría de las denegaciones de acceso indican que SELinux funciona correctamente al bloquear acciones incorrectas.
- La evaluación de las acciones denegadas requiere cierta familiaridad con las acciones de servicio normales y esperadas.
- El problema más frecuente de SELinux es un contexto de archivos incorrecto en archivos nuevos, copiados o movidos.
- Los contextos de archivos se corrigen fácilmente cuando una política existente hace referencia a su ubicación.
- Las características opcionales de la política booleana están documentadas en las páginas del manual `_selinux`.
- La implementación de funciones booleanas generalmente requiere establecer una configuración adicional que no sea de SELinux.
- Las políticas de SELinux no reemplazan ni eluden los permisos de archivos o las restricciones de la lista de control de acceso.

Cuando una aplicación o servicio común falla, y se sabe que el servicio tiene una política de SELinux en funcionamiento, primero revise la página del manual `_selinux` del servicio para

verificar la etiqueta de tipo de contexto correcta. Vea el proceso afectado y los atributos del archivo para verificar que se definan las etiquetas correctas.

Monitoreo de las violaciones de SELinux

El servicio de solución de problemas de SELinux, del paquete `setroubleshoot-server` brinda herramientas para diagnosticar problemas de SELinux. Cuando SELinux rechaza una acción, se registra un mensaje de caché de vector de acceso (AVC) en el archivo de registro de seguridad `/var/log/audit/audit.log`. El servicio de solución de problemas de SELinux monitorea los eventos de AVC y envía un resumen de eventos al archivo `/var/log/messages`.

El resumen de AVC incluye un identificador único de evento (UUID). Use el comando `sealert -l UUID` para ver los detalles completos del informe para el evento específico. Use el comando `sealert -a /var/log/audit/audit.log` para ver todos los eventos existentes.

Considere el siguiente ejemplo de secuencia de comandos en un servidor web Apache estándar: Puede crear `/root/mypage` y moverlo a la carpeta predeterminada de contenido de Apache (`/var/www/html`). A continuación, después de iniciar el servicio Apache, intente recuperar el contenido del archivo.

```
[root@host ~]# touch /root/mypage
[root@host ~]# mv /root/mypage /var/www/html
[root@host ~]# systemctl start httpd
[root@host ~]# curl http://localhost/mypage
<!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 this resource.</p>
</body></html>
```

El servidor web no muestra el contenido y devuelve un error `permission denied`. Se registra un evento de AVC en los archivos `/var/log/audit/audit.log` y `/var/log/messages`. Observe el comando `sealert` sugerido y el UUID en el mensaje de evento `/var/log/messages`.

```
[root@host ~]# tail /var/log/audit/audit.log
...output omitted...
type=AVC msg=audit(1649249057.067:212): avc: denied { getattr }
for pid=2332 comm="httpd" path="/var/www/html/mypage"
dev="vda4" ino=9322502 scontext=system_u:system_r:httpd_t:s0
tcontext=unconfined_u:object_r:admin_home_t:s0 tclass=file permissive=0
...output omitted
[root@host ~]# tail /var/log/messages
...output omitted...
Apr  6 08:44:19 host setroubleshoot[2547]: SELinux is preventing /usr/sbin/httpd
from getattr access on the file /var/www/html/mypage. For complete SELinux
messages run: sealert -l 95f41f98-6b56-45bc-95da-ce67ec9a9ab7
...output omitted...
```

La salida `sealert` describe el evento, incluido el proceso afectado, el archivo al que se accedió y la acción intentada y denegada. La salida incluye consejos para corregir la etiqueta del archivo, si corresponde. Los consejos adicionales describen cómo generar una nueva política para permitir la acción denegada. Use los consejos proporcionados solo cuando sea adecuado para su situación.

**Importante**

La salida `sealert` incluye una calificación de confianza, que indica el nivel de confianza de que el consejo dado mitigará la denegación. Sin embargo, es posible que ese consejo no sea adecuado para su situación.

Por ejemplo, si la denegación de AVC se debe a que el archivo denegado se encuentra en la ubicación incorrecta, el consejo que indica que se debe ajustar la etiqueta de contexto del archivo o crear una nueva política para esta ubicación y acción es técnicamente correcto, pero no es el correcto para su situación. Si la causa raíz es una ubicación o nombre de archivo incorrectos, entonces la solución adecuada es mover o cambiar el nombre del archivo y luego restaurar un contexto de archivo correcto.

```
[root@host ~]# sealert -l 95f41f98-6b56-45bc-95da-ce67ec9a9ab7
SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/mypage.

***** Plugin restorecon (99.5 confidence) suggests *****

If you want to fix the label.
/var/www/html/mypage default label should be httpd_sys_content_t.
Then you can run restorecon. The access attempt may have been stopped due to
insufficient permissions to access a parent directory in which case try to change
the following command accordingly.
Do
# /sbin/restorecon -v /var/www/html/mypage

***** Plugin catchall (1.49 confidence) suggests *****

If you believe that httpd should be allowed getattr access on the mypage 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:
# ausearch -c 'httpd' --raw | audit2allow -M my-httpd
# semodule -X 300 -i my-httpd.pp

Additional Information:
Source Context          system_u:system_r:httpd_t:s0
Target Context          unconfined_u:object_r:admin_home_t:s0
Target Objects          /var/www/html/mypage [ file ]
Source                 httpd
Source Path             /usr/sbin/httpd
...output omitted...

Raw Audit Messages
type=AVC msg=audit(1649249057.67:212): avc: denied { getattr }
for pid=2332 comm="httpd" path="/var/www/html/mypage"
dev="vda4" ino=9322502 scontext=system_u:system_r:httpd_t:s0
tcontext=unconfined_u:object_r:admin_home_t:s0 tclass=file permissive=0
```

```

type=SYSCALL msg=audit(1649249057.67:212): arch=x86_64 syscall=newfstatat
  success=no exit=EACCES a0=fffffff9c a1=7fe9c00048f8 a2=7fe9ccfc8830 a3=100
  items=0 ppid=2329 pid=2332 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,admin_home_t,file,getattr

```

En este ejemplo, el archivo al que se accedió está en la ubicación correcta, pero no tiene el contexto de archivo SELinux correcto. La sección Raw Audit Messages muestra información de la entrada del evento /var/log/audit.log. Use el comando `restorecon /var/www/html/mypage` para definir la etiqueta de contexto correcta. Para corregir varios archivos de manera recursiva, use el comando `restorecon -R` en el directorio principal.

Use el comando `ausearch` para buscar eventos de AVC en el archivo de registro /var/log/audit.log. Use la opción `-m` para especificar el tipo de mensaje AVC y la opción `-ts` para proporcionar una sugerencia de tiempo, como `recent`.

```

[root@host ~]# ausearch -m AVC -ts recent
-----
time->Tue Apr  6 13:13:07 2019
type=PROCTITLE msg=audit(1554808387.778:4002):
  proctitle=2F7573722F7362696E2F6874747064002D44464F524547524F554E44
type=SYSCALL msg=audit(1554808387.778:4002): arch=c000003e syscall=49
  success=no exit=-13 a0=3 a1=55620b8c9280 a2=10 a3=7ffed967661c items=0
  ppid=1 pid=9340 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0
  sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="httpd" exe="/usr/sbin/httpd"
  subj=system_u:system_r:httpd_t:s0 key=(null)
type=AVC msg=audit(1554808387.778:4002): avc: denied { name_bind }
  for pid=9340 comm="httpd" src=82 scontext=system_u:system_r:httpd_t:s0
  tcontext=system_u:object_r:reserved_port_t:s0 tclass=tcp_socket permissive=0

```

Solución de problemas de SELinux con la consola web

La consola web de RHEL incluye herramientas para solucionar problemas de SELinux. Seleccione SELinux del menú a la izquierda. La ventana de política de SELinux muestra el estado de cumplimiento (enforcing) actual. La sección SELinux access control errors enumera los problemas actuales de SELinux.

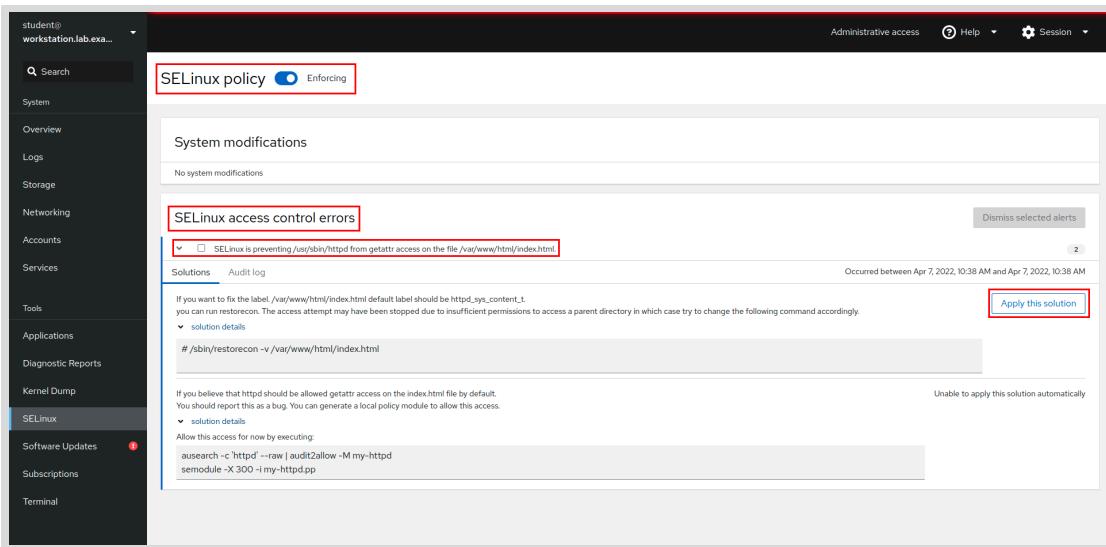


Figura 5.3: Política de SELinux y errores en la consola web

Haga clic en el carácter > para mostrar los detalles del evento. Haga clic en **solution details** (detalles de la solución) para mostrar todos los detalles y consejos del evento. Puede hacer clic en **Apply the solution** (Aplicar la solución) para aplicar los consejos dados.

Después de corregir el problema, en la sección **SELinux access control errors**, se deberá eliminar ese evento de la vista. Si aparece el mensaje **No SELinux alerts**, significa que ha corregido todos los problemas actuales de SELinux.



Referencias

Página del manual: `sealert(8)`

► Ejercicio Guiado

Investigación y resolución de problemas de SELinux

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

Resultados

- Obtenga experiencia con las herramientas para la solución de problemas de SELinux.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start selinux-issues
```

Instrucciones

- 1. Desde un navegador web en la máquina `workstation`, abra la página web `http://servera/index.html`. Un mensaje de error indica que no tiene permiso para acceder al archivo.
- 2. Use el comando `ssh` para iniciar sesión en `servera` con el usuario `student`. Use el comando `sudo -i` para cambiar al usuario `root`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

- 3. Use el comando `less` para visualizar el contenido del archivo `/var/log/messages`. Use el carácter `/` y busque el texto `sealert`. Presione la tecla `n` hasta llegar a la última aparición, ya que los ejercicios anteriores también pueden haber generado mensajes de SELinux. Copie el comando `sealert` sugerido para que pueda usarlo en el siguiente paso. Use la tecla `q` para salir del comando `less`.

```
[root@servera ~]# less /var/log/messages
...output omitted...
Apr  7 04:52:18 servera setroubleshoot[20715]: SELinux is preventing /usr/sbin/
httpd from getattr access on the file /custom/index.html. For complete SELinux
messages run: sealert -l 9a96294a-239b-4568-8f1e-9f35b5fb472b
...output omitted...
```

- 4. Ejecute el comando sugerido `sealert`. Tenga en cuenta el contexto de origen, los objetos de destino, la política y el modo de cumplimiento (enforcing). Busque la etiqueta de contexto SELinux correcta para el archivo que el servicio `httpd` intenta proporcionar.

4.1. Ejecute el comando `sealert`.

La salida explica que el archivo `/custom/index.html` tiene una etiqueta de contexto incorrecta.

```
[root@servera ~]# sealert -l 9a96294a-239b-4568-8f1e-9f35b5fb472b
SELinux is preventing /usr/sbin/httpd from getattr access on the file /custom/
index.html.

***** Plugin catchall_labels (83.8 confidence) suggests *****

If you want to allow httpd to have getattr access on the index.html file
Then you need to change the label on /custom/index.html
Do
# semanage fcontext -a -t FILE_TYPE '/custom/index.html'
where FILE_TYPE is one of the following: NetworkManager_exec_t,
NetworkManager_log_t, NetworkManager_tmp_t, abrt_dump_oops_exec_t,
abrt_etc_t, abrt_exec_t, abrt_handle_event_exec_t, abrt_helper_exec_t,
abrt_retrace_coredump_exec_t, abrt_retrace_spool_t, abrt_retrace_worker_exec_t,
abrt_tmp_t, abrt_upload_watch_tmp_t, abrt_var_cache_t, abrt_var_log_t,
abrt_var_run_t, accountsd_exec_t, acct_data_t, acct_exec_t, admin_crontab_tmp_t,
admin_passwd_exec_t, afs_logfile_t, aide_exec_t, aide_log_t, alsa_exec_t,
alsa_tmp_t, amanda_exec_t, amanda_log_t, amanda_recover_exec_t, amanda_tmp_t,
amtu_exec_t, anacron_exec_t, anon_inodefs_t
...output omitted...

Additional Information:
Source Context          system_u:system_r:httpd_t:s0
Target Context          unconfined_u:object_r:default_t:s0
Target Objects          /custom/index.html [ file ]
Source                 httpd
Source Path             /usr/sbin/httpd
Port                  <Unknown>
Host                  servera.lab.example.com
Source RPM Packages    httpd-2.4.51-7.el9_0.x86_64
Target RPM Packages    selinux-policy-targeted-34.1.27-1.el9.noarch
SELinux Policy RPM     selinux-policy-targeted-34.1.27-1.el9.noarch
Local Policy RPM       True
Selinux Enabled         targeted
Policy Type            Enforcing
Enforcing Mode         Enforcing
Host Name              servera.lab.example.com
Platform               Linux servera.lab.example.com
                        5.14.0-70.2.1.el9_0.x86_64 #1 SMP PREEMPT Wed Mar
                        16 18:15:38 EDT 2022 x86_64 x86_64
Alert Count            4
First Seen             2022-04-07 04:51:38 EDT
Last Seen              2022-04-07 04:52:13 EDT
Local ID               9a96294a-239b-4568-8f1e-9f35b5fb472b

Raw Audit Messages
```

capítulo 5 | Administración de seguridad de SELinux

```
type=AVC msg=audit(1649321533.406:1024): avc: denied { setattr } for
pid=20464 comm="httpd" path="/custom/index.html" dev="vda4" ino=25571802
scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:default_t:s0
tclass=file permissive=0

...output omitted...
```

- 4.2. Verifique el contexto de SELinux para el directorio desde donde el servicio httpd proporciona el contenido de manera predeterminada, /var/www/html. El contexto de SELinux httpd_sys_content_t es apropiado para el archivo /custom/index.html.

```
[root@servera ~]# ls -ldz /var/www/html
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Mar 21 11:47 /
var/www/html
```

- 5. La sección Raw Audit Messages del comando sealert contiene información del archivo /var/log/audit/audit.log. Use el comando ausearch para buscar el archivo /var/log/audit/audit.log. La opción -m busca en el tipo de mensaje. La opción -ts busca en función del tiempo. La siguiente entrada identifica el proceso relevante y el archivo que causa la alerta. El proceso es el servidor web Apache httpd, el archivo es /custom/index.html y el contexto es system_r:httpd_t.

```
[root@servera ~]# ausearch -m AVC -ts today
...output omitted...
-----
time->Thu Apr  7 04:52:13 2022
type=PROCTITLE msg=audit(1649321533.406:1024):
    proctitle=2F7573722F7362696E2F6874747064002D44464F524547524F554E44
type=SYSCALL msg=audit(1649321533.406:1024): arch=c000003e syscall=262 success=no
    exit=-13 a0=ffffffff9c a1=7fefc403d850 a2=7fefc89bc830 a3=100 items=0 ppid=20461
    pid=20464 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)
type=AVC msg=audit(1649321533.406:1024): avc: denied
    { setattr } for pid=20464 comm="httpd" path="/custom/index.html"
    dev="vda4" ino=25571802 scontext=system_u:system_r:httpd_t:s0
    tcontext=unconfined_u:object_r:default_t:s0 tclass=file permissive=0
```

- 6. Resuelva el problema aplicando el contexto httpd_sys_content_t.

```
[root@servera ~]# semanage fcontext -a \
-t httpd_sys_content_t '/custom(/.*)?'
[root@servera ~]# restorecon -Rv /custom
Relabeled /custom from unconfined_u:object_r:default_t:s0 to
unconfined_u:object_r:httpd_sys_content_t:s0
Relabeled /custom/index.html from unconfined_u:object_r:default_t:s0 to
unconfined_u:object_r:httpd_sys_content_t:s0
```

- 7. Nuevamente, intente visualizar http://servera/index.html. Se muestra el mensaje This is SERVERA..

- 8. Regrese a la máquina **workstation** como el usuario **student**.

```
[root@servera ~]# exit  
logout  
[student@servera ~]$ exit  
logout  
Connection to servera closed.  
[student@workstation ~]$
```

Finalizar

En la máquina **workstation**, cambie al directorio de inicio de usuario **student** y use el comando **lab** para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish selinux-issues
```

Esto concluye la sección.

► Trabajo de laboratorio

Administración de seguridad de SELinux

En este trabajo de laboratorio, identificará problemas en los archivos de registro del sistema y ajustará la configuración de SELinux.

Resultados

- Identificar problemas en los archivos de registro del sistema.
- Ajustar la configuración de SELinux.

Antes De Comenzar

Con el usuario **student** en la máquina **workstation**, use el comando **lab** para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start selinux-review
```

Instrucciones

1. Inicie sesión en la máquina **serverb** como el usuario **student** y cambie al usuario **root**.
2. Desde un navegador web en la máquina **workstation**, vea la página web <http://serverb/lab.html>. Debe ver el siguiente mensaje de error: You do not have permission to access this resource.
3. Investigue e identifique el problema de SELinux que impide que el servicio Apache proporcione el contenido web.
4. Muestre el contexto de SELinux del nuevo directorio de documentos HTTP y el directorio de documentos HTTP original. Resuelva el problema de SELinux que evita que el servidor Apache proporcione el contenido web.
5. Verifique que el servidor Apache ahora pueda proporcionar contenido web.
6. Regrese a la máquina **workstation** como el usuario **student**.

Evaluación

Con el usuario **student** en la máquina **workstation**, use el comando **lab** para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade selinux-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish selinux-review
```

Esto concluye la sección.

► Solución

Administración de seguridad de SELinux

En este trabajo de laboratorio, identificará problemas en los archivos de registro del sistema y ajustará la configuración de SELinux.

Resultados

- Identificar problemas en los archivos de registro del sistema.
- Ajustar la configuración de SELinux.

Antes De Comenzar

Con el usuario **student** en la máquina **workstation**, use el comando **lab** para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start selinux-review
```

Instrucciones

- Inicie sesión en la máquina **serverb** como el usuario **student** y cambie al usuario **root**.

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
[student@serverb ~]$ sudo -i
[sudo] password for student: student
[root@serverb ~]#
```

- Desde un navegador web en la máquina **workstation**, vea la página web <http://serverb/lab.html>. Debe ver el siguiente mensaje de error: You do not have permission to access this resource.
- Investigue e identifique el problema de SELinux que impide que el servicio Apache proporcione el contenido web.
 - Vea el contenido del archivo **/var/log/messages**. Use la tecla / y busque la cadena **sealert**. Use la tecla q para salir del comando **less**.

```
[root@serverb ~]# less /var/log/messages
...output omitted...
Apr  7 06:16:15 serverb setroubleshoot[26509]: failed to retrieve rpm info for /
lab-content/la
b.html
Apr  7 06:16:17 serverb setroubleshoot[26509]: SELinux is preventing /usr/sbin/
httpd from getattr access on the file /lab-content/lab.html. For complete SELinux
messages run: sealert -l 35c9e452-2552-4ca3-8217-493b72ba6d0b
Apr  7 06:16:17 serverb setroubleshoot[26509]: SELinux is preventing /usr/sbin/
httpd from getattr access on the file /lab-content/lab.html
...output omitted...
```

- 3.2. Ejecute el comando sugerido `sealert`. Tenga en cuenta el contexto de origen, los objetos de destino, la política y el modo de cumplimiento (enforcing).

```
[root@serverb ~]# sealert -l 35c9e452-2552-4ca3-8217-493b72ba6d0b
SELinux is preventing /usr/sbin/httpd from getattr access on the file /lab-
content/lab.html.

***** Plugin catchall_labels (83.8 confidence) suggests *****

If you want to allow httpd to have getattr access on the lab.html file
Then you need to change the label on /lab-content/lab.html
Do
# semanage fcontext -a -t FILE_TYPE '/lab-content/lab.html'
where FILE_TYPE is one of the following:
...output omitted...

Additional Information:
Source Context          system_u:system_r:httpd_t:s0
Target Context          unconfined_u:object_r:default_t:s0
Target Objects          /lab-content/lab.html [ file ]
Source                 httpd
Source Path             /usr/sbin/httpd
Port                   <Unknown>
Host                  serverb.lab.example.com
Source RPM Packages    httpd-2.4.51-7.el9_0.x86_64
Target RPM Packages    selinux-policy-targeted-34.1.27-1.el9.noarch
SELinux Policy RPM     selinux-policy-targeted-34.1.27-1.el9.noarch
Local Policy RPM       True
Selinux Enabled         targeted
Policy Type            Enforcing
Enforcing Mode         serverb.lab.example.com
Host Name              Linux serverb.lab.example.com
Platform               5.14.0-70.2.1.el9_0.x86_64 #1 SMP PREEMPT Wed Mar
16 18:15:38 EDT 2022 x86_64 x86_64
Alert Count             8
First Seen              2022-04-07 06:14:45 EDT
Last Seen               2022-04-07 06:16:12 EDT
Local ID                35c9e452-2552-4ca3-8217-493b72ba6d0b

Raw Audit Messages
```

capítulo 5 | Administración de seguridad de SELinux

```
type=AVC msg=audit(1649326572.86:407): avc: denied { setattr } for
pid=10731 comm="httpd" path="/lab-content/lab.html" dev="vda4" ino=18192752
scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:default_t:s0
tclass=file permissive=0

type=SYSCALL msg=audit(1649326572.86:407): arch=x86_64 syscall=newfstatat
success=no exit=EACCES a0=fffffff9c a1=7f7c8c0457c0 a2=7f7c887f7830 a3=100 items=0
ppid=10641 pid=10731 auid=4294967295 uid=48 gid=48 euid=48 suid=48 fsuid=48
egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 comm=httpd exe=/usr/sbin/httpd
subj=system_u:system_r:httpd_t:s0 key=(null)

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

- 3.3. La sección Raw Audit Messages del comando `sealert` contiene información del archivo `/var/log/audit/audit.log`. Busque el archivo `/var/log/audit/audit.log`. La opción `-m` busca en el tipo de mensaje. La opción `-ts` busca en función del tiempo. La siguiente entrada identifica el proceso relevante y el archivo que causa la alerta. El proceso es el servidor web Apache `httpd`, el archivo es `/lab-content/lab.html` y el contexto es `system_r:httpd_t`.

```
[root@serverb ~]# ausearch -m AVC -ts recent
...output omitted...
---

time->Thu Apr  7 06:16:12 2022
type=PROCTITLE msg=audit(1649326572.086:407):
proctitle=2F7573722F7362696E2F6874747064002D44464F524547524F554E44
type=SYSCALL msg=audit(1649326572.086:407): arch=c000003e syscall=262 success=no
exit=-13 a0=fffffff9c a1=7f7c8c0457c0 a2=7f7c887f7830 a3=100 items=0 ppid=10641
pid=10731 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)
type=AVC msg=audit(1649326572.086:407): avc: denied { setattr } for
pid=10731 comm="httpd" path="/lab-content/lab.html" dev="vda4" ino=18192752
scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:default_t:s0
tclass=file permissive=0
```

4. Muestre el contexto de SELinux del nuevo directorio de documentos HTTP y el directorio de documentos HTTP original. Resuelva el problema de SELinux que evita que el servidor Apache proporcione el contenido web.

- 4.1. Compare el contexto de SELinux para los directorios `/lab-content` y `/var/www/html`.

```
[root@serverb ~]# ls -dz /lab-content /var/www/html
unconfined_u:object_r:default_t:s0 /lab-content
system_u:object_r:httpd_sys_content_t:s0 /var/www/html
```

- 4.2. Cree una regla de contextos de archivos que establezca el tipo predeterminado en `httpd_sys_content_t` para el directorio `/lab-content` y todos los archivos en él.

```
[root@serverb ~]# semanage fcontext -a \
-t httpd_sys_content_t '/lab-content(/.*)?'
```

- 4.3. Corrija el contexto de SELinux para los archivos en el directorio /lab-content.

```
[root@serverb ~]# restorecon -R /lab-content/
```

5. Verifique que el servidor Apache ahora pueda proporcionar contenido web.

- 5.1. Use su navegador web para actualizar el enlace http://serverb/lab.html. Si se muestra el contenido, su problema está resuelto.

```
This is the html file for the SELinux final lab on SERVERB.
```

6. Regrese a la máquina workstation como el usuario student.

```
[root@serverb ~]# exit  
logout  
[student@serverb ~]$ exit  
logout  
Connection to serverb closed.  
[student@workstation ~]$
```

Evaluación

Con el usuario student en la máquina workstation, use el comando lab para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade selinux-review
```

Finalizar

En la máquina workstation, cambie al directorio de inicio de usuario student y use el comando lab para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish selinux-review
```

Esto concluye la sección.

Resumen

- Use los comandos `getenforce` y `setenforce` para administrar el modo de SELinux de un sistema.
- El comando `semanage` administra las reglas de políticas de SELinux. El comando `restorecon` aplica el contexto que define la política.
- Los booleanos son opciones que modifican el comportamiento de la política de SELinux. Puede habilitarlos o deshabilitarlos para ajustar la política.
- El comando `sealert` muestra información útil que ayuda con la solución de problemas de SELinux.

capítulo 6

Ajuste del rendimiento del sistema

Meta

Evalúe y controle procesos, establezca parámetros de ajuste y adapte las prioridades de programación de procesos en un sistema Red Hat Enterprise Linux.

Objetivos

- Usar comandos para finalizar procesos y comunicarse con ellos, definir las características de un proceso daemon y detener sesiones y procesos de usuario.
- Definir el promedio de carga y determinar los procesos del servidor que consumen muchos recursos.
- Optimizar el rendimiento del sistema seleccionando un perfil de ajuste administrado por el daemon.
- Dar o quitar la prioridad a procesos específicos con los comandos nice y renice.

Secciones

- Finalización de procesos (y ejercicio guiado)
- Monitoreo de actividades del proceso (y ejercicio guiado)
- Ajuste de perfiles de optimización (y ejercicio guiado)
- Influencia en la programación de procesos (y ejercicio guiado)

Trabajo de laboratorio

- Ajuste del rendimiento del sistema

Finalización de procesos

Objetivos

Usar comandos para finalizar procesos y comunicarse con ellos, definir las características de un proceso daemon y detener 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 (una solicitud de entrada o salida o un temporizador vencido), o el uso explícito de un comando emisor de señal o secuencia de teclado.

En la siguiente tabla, se enumeran 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

Señal	Nombre	Definición
1	HUP	Hangup : Se usa para informar la finalización del proceso de control de un terminal. Además, solicita que se reinicie el proceso (volver a cargar la configuración) sin finalización.
2	INT	Keyboard interrupt : Provoca la finalización del programa. Puede bloquearse o manipularse. Enviado al presionar la secuencia de teclas INTR (Interrumpir) (Ctrl+c).
3	QUIT	Keyboard quit : Es similar a SIGINT, pero añade el volcado de un proceso en la finalización. Enviado al presionar una secuencia de teclas QUIT (kbd:[Ctrl+\]).
9	KILL	Kill, unblockable : Provoca la finalización abrupta del programa. No se puede bloquear, ignorar ni manipular; sistemáticamente es grave.
15 predeter	TERM	Terminate : Provoca la finalización del programa. A diferencia de SIGKILL, puede bloquearse, ignorarse o manipularse. La forma "limpia" de solicitar la finalización de un programa; permite que el programa complete las operaciones esenciales y la autolimpieza antes de la finalización.
18	CONT	Continue : Se envía a un proceso para que se reinicie, en caso de que esté detenido. No puede bloquearse. Aún si se manipula, reinicia siempre el proceso.
19	STOP	Stop, unblockable : Suspende el proceso. No puede bloquearse o manipularse.

Señal	Nombre	Definición
20	TSTP	Keyboard stop : A diferencia de SIGSTOP, puede bloquearse, ignorarse o manipularse. Enviado al presionar una secuencia de teclas de suspensión (Ctrl+z).

**nota**

Los números de señal varían en las distintas plataformas de hardware de Linux, pero los nombres y los significados están estandarizados. Se recomienda usar nombres de señales en lugar de números al realizar la señalización. Los números analizados en esta sección son para los sistemas con arquitectura x86_64.

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 [core]) y que, a continuación, finalice.
- **Stop** : Provoca que un programa deje de ejecutarse (se suspenda) y espere para continuar (se reinicie).

Los programas reaccionan ante señales de eventos esperadas mediante la implementación de rutinas de controlador que ignoren, reemplacen o amplíen la acción predeterminada de una señal.

Envío de señales mediante una solicitud explícita

Puede indicar 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 (core) (Ctrl +\) del proceso. Sin embargo, usará comandos emisores de señales para enviar señales a un proceso en segundo plano de una sesión diferente.

Las señales se pueden especificar por nombre (por ejemplo, -HUP o -SIGHUP) o por número (la opción -1 relacionada). Los usuarios pueden finalizar sus procesos, pero se necesitan privilegios de root para finalizar procesos que son propiedad de otros usuarios.

El comando `kill` usa un número PID para enviar una señal a un proceso. A pesar de su nombre, el comando `kill` puede usarse para enviar cualquier señal y no solo aquellas para finalizar programas. Puede usar el comando `kill` con la opción -l para enumerar los nombres y números de todas las señales disponibles.

```
[user@host ~]$ kill -l
 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 omitted...
[user@host ~]$ ps aux | grep job
5194 0.0 0.1 222448 2980 pts/1 S 16:39 0:00 /bin/bash /home/user/bin/control job1
5199 0.0 0.1 222448 3132 pts/1 S 16:39 0:00 /bin/bash /home/user/bin/control job2
5205 0.0 0.1 222448 3124 pts/1 S 16:39 0:00 /bin/bash /home/user/bin/control job3
5430 0.0 0.0 221860 1096 pts/1 S+ 16:41 0:00 grep --color=auto job
[user@host ~]$ kill 5194
[user@host ~]$ ps aux | grep job
```

```

user  5199  0.0  0.1 222448  3132 pts/1    S    16:39   0:00 /bin/bash /home/
user/bin/control job2
user  5205  0.0  0.1 222448  3124 pts/1    S    16:39   0:00 /bin/bash /home/
user/bin/control job3
user  5783  0.0  0.0 221860   964 pts/1    S+   16:43   0:00 grep --color=auto
job
[1]  Terminated                  control job1
[user@host ~]$ kill -9 5199
[user@host ~]$ ps aux | grep job
user  5205  0.0  0.1 222448  3124 pts/1    S    16:39   0:00 /bin/bash /home/
user/bin/control job3
user  5930  0.0  0.0 221860  1048 pts/1    S+   16:44   0:00 grep --color=auto
job
[2]- Killed                     control job2
[user@host ~]$ kill -SIGTERM 5205
user  5986  0.0  0.0 221860  1048 pts/1  S+  16:45   0:00 grep --color=auto job
[3]+ Terminated                 control job3

```

El comando `killall` puede señalar varios procesos según su nombre de comando.

```

[user@host ~]$ ps aux | grep job
5194  0.0  0.1 222448  2980 pts/1    S    16:39   0:00 /bin/bash /home/user/bin/
control job1
5199  0.0  0.1 222448  3132 pts/1    S    16:39   0:00 /bin/bash /home/user/bin/
control job2
5205  0.0  0.1 222448  3124 pts/1    S    16:39   0:00 /bin/bash /home/user/bin/
control job3
5430  0.0  0.0 221860  1096 pts/1    S+   16:41   0:00 grep --color=auto job
[user@host ~]$ killall control
[1]  Terminated                  control job1
[2]- Terminated                 control job2
[3]+ Terminated                 control job3
[user@host ~]$ 

```

Use el comando `pkill` para enviar una señal a uno o más procesos que coincidan con los criterios de selección. Los criterios de selección pueden ser un nombre de comando, un proceso que es propiedad de un usuario específico o todos los procesos del sistema. El comando `pkill` incluye criterios de selección avanzados:

- **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 una terminal de control específica.

```

[user@host ~]$ ps aux | grep pkill
user  5992  0.0  0.1 222448  3040 pts/1    S    16:59   0:00 /bin/bash /home/
user/bin/control pkill1
user  5996  0.0  0.1 222448  3048 pts/1    S    16:59   0:00 /bin/bash /home/
user/bin/control pkill2
user  6004  0.0  0.1 222448  3048 pts/1    S    16:59   0:00 /bin/bash /home/
user/bin/control pkill3
[user@host ~]$ pkill control
[1]  Terminated                  control pkill1

```

```
[2]- Terminated control pkill2
[user@host ~]$ ps aux | grep pkill
user  6219  0.0  0.0 221860  1052 pts/1    S+   17:00   0:00 grep --color=auto
pkill
[3]+ Terminated control pkill3
[user@host ~]$ ps aux | grep test
user  6281  0.0  0.1 222448  3012 pts/1    S    17:04   0:00 /bin/bash /home/
user/bin/control test1
user  6285  0.0  0.1 222448  3128 pts/1    S    17:04   0:00 /bin/bash /home/
user/bin/control test2
user  6292  0.0  0.1 222448  3064 pts/1    S    17:04   0:00 /bin/bash /home/
user/bin/control test3
user  6318  0.0  0.0 221860  1080 pts/1    S+   17:04   0:00 grep --color=auto
test
[user@host ~]$ pkill -U user
[user@host ~]$ ps aux | grep test
user  6870  0.0  0.0 221860  1048 pts/0    S+   17:07   0:00 grep --color=auto
test
```

Usuarios de cierre de sesión administrativo

Es posible que deba cerrar la sesión de otros usuarios por diversos motivos. Algunos escenarios posibles: el usuario cometió una infracción de seguridad; el usuario puede haber abusado de los recursos; el usuario puede tener un sistema que no responde; o el usuario tiene acceso inadecuado a los materiales. En estos casos, debe finalizar su sesión mediante el uso de señales de forma administrativa.

Primero, para cerrar la sesión de un usuario, identifique la sesión de inicio de sesión que se finalizará. Use el comando `w` para enumerar los inicios de sesión de usuario y los procesos actuales en ejecución. Observe las columnas TTY y FROM para determinar las sesiones a cerrar.

Todas las sesiones de inicio de sesión de usuario están asociadas a un dispositivo terminal (TTY). Si el nombre del dispositivo es `pts/N`, se trata de una *pseudoterminal* asociada con una ventana de terminal gráfica o sesión de inicio de sesión remota. Si es `ttyN`, el usuario se encuentra en una consola del sistema, consola alternativa u otro dispositivo terminal conectado directamente.

```
[user@host ~]$ w
12:43:06 up 27 min,  5 users,  load average: 0.03, 0.17, 0.66
USER     TTY      FROM          LOGIN@    IDLE    JCPU   PCPU WHAT
root     tty2          12:26   14:58   0.04s  0.04s -bash
bob      tty3          12:28   14:42   0.02s  0.02s -bash
user     pts/1  desktop.example.com 12:41   2.00s  0.03s  0.03s w
[user@host ~]$
```

Averigüe cuánto tiempo un usuario estuvo en el sistema con la hora de inicio de 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 para cada sesión. El consumo de CPU del proceso de primer plano actual está en la columna PCPU.

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 los procesos y shells de inicio de sesión de un usuario requiere de la señal SIGKILL.

**Importante**

Los administradores suelen usar SIGKILL.

Siempre es grave porque la señal SIGKILL no puede manipularse ni ignorarse.

Sin embargo, obliga a la finalización sin permitir que el proceso terminado ejecute rutinas de autolimpieza. Red Hat recomienda enviar primero SIGTERM, a continuación intentar con SIGINT y, solo si falla en ambos casos, intentar con SIGKILL.

Primero, use el comando `pgrep` para identificar los números de PID que desea eliminar. Este comando funciona de manera similar al comando `pkill`, incluidas las mismas opciones, excepto que el comando `pgrep` enumera los procesos en lugar de eliminarlos.

```
[root@host ~]# pgrep -l -u bob
6964 bash
6998 sleep
6999 sleep
7000 sleep
[root@host ~]# pkill -SIGKILL -u bob
[root@host ~]# pgrep -l -u bob
```

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. Use el comando `w` para determinar la terminal de control para la sesión y, a continuación, finalice solo los procesos con 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@host ~]# pgrep -l -u bob
7391 bash
7426 sleep
7427 sleep
7428 sleep
[root@host ~]# w -h -u bob
bob      tty3      18:37      5:04    0.03s  0.03s -bash
[root@host ~]# pkill -t tty3
[root@host ~]# pgrep -l -u bob
7391 bash
[root@host ~]# pkill -SIGKILL -t tty3
[root@host ~]# pgrep -l -u bob
[root@host ~]#
```

Puede aplicar 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 hayan creado. Esta vez, la shell de inicio de sesión Bash principal sobrevive porque la señal se dirige solo a sus procesos secundarios.

```
[root@host ~]# pstree -p bob
bash(8391)─sleep(8425)
              └─sleep(8426)
```

```
└─sleep(8427)
[root@host ~]# pkill -P 8391
[root@host ~]# pgrep -l -u bob
bash(8391)
[root@host ~]# pkill -SIGKILL -P 8391
[root@host ~]# pgrep -l -u bob
bash(8391)
```



Referencias

Páginas del manual: `kill(1)`, `killall(1)`, `pgrep(1)`, `pkill(1)`, `pstree(1)`,
`signal(7)` y `w(1)`

Para efectuar lecturas complementarias, consulte *Signal Handling* en
<https://www.gnu.org/software/libc/manual/pdf/libc.pdf#Signal%20Handling>

Para efectuar lecturas complementarias, consulte *Processes* en
<https://www.gnu.org/software/libc/manual/pdf/libc.pdf#Processes>

► Ejercicio Guiado

Finalización de procesos

En este ejercicio, usa señales para gestionar y detener procesos.

Resultados

- Iniciar y detener varios procesos de shell.

Antes De Comenzar

Con el usuario **student** en la máquina **workstation**, use el comando **lab** para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start processes-kill
```

Instrucciones

- 1. En la máquina **workstation**, abra dos ventanas de terminal, una al lado de la otra. En esta sección, estas terminales se denominan *izquierda* y *derecha*. En cada terminal, use el comando **ssh** para iniciar sesión en la máquina **servera** como el usuario **student**.

```
[student@workstation ~]$ ssh student@servera
[student@servera ~]$
```

- 2. En la shell de terminal izquierda, cree el directorio **/home/student/bin**. Cree el script de shell **instance** en el nuevo directorio. Cambie los permisos del script para que sea ejecutable.

2.1. Cree el directorio **/home/student/bin**.

```
[student@servera ~]$ mkdir /home/student/bin
```

2.2. Cree el archivo de script **instance** en el directorio **/home/student/bin**. Presione la tecla **i** para ingresar al modo interactivo Vim. El archivo debe tener el siguiente contenido, como se muestra. Use el comando **:wq** para guardar el archivo.

```
[student@servera ~]$ cd /home/student/bin
[student@servera bin]$ vim /home/student/bin/instance
#!/bin/bash
while true; do
    echo -n "$@" >> ~/instance_outfile
    sleep 5
done
```

**nota**

El script `instance` se ejecuta hasta que el proceso se termine. Adjunta argumentos de línea de comandos al archivo `~/instance_outfile` una vez cada 5 segundos.

- 2.3. Haga el archivo de script `instance` ejecutable.

```
[student@servera ~]$ chmod +x /home/student/bin/instance
```

- 3. En la shell de terminal izquierda, cambie al directorio `/home/student/bin/`. Inicie tres procesos con el archivo de script `instance`, pasando los argumentos `network`, `interface` y `connection`. Inicie los procesos en segundo plano.

```
[student@servera bin]$ instance network &
[1] 3460
[student@servera bin]$ instance interface &
[2] 3482
[student@servera bin]$ instance connection &
[3] 3516
```

- 4. En la shell de terminal derecha, verifique que los tres procesos se estén adjuntando al archivo `~/home/student/instance_outfile`.

```
[student@servera ~]$ tail -f ~/instance_outfile
network interface network connection interface network connection interface
network
...output omitted...
```

- 5. En la shell de terminal izquierda, enumere los trabajos existentes.

```
[student@servera bin]$ jobs
[1]  Running           instance network &
[2]- Running           instance interface &
[3]+ Running           instance connection &
```

- 6. Use señales para suspender el proceso `instance network`. Verifique que el proceso `instance network` esté configurado como Stopped. Verifique que el proceso `network` ya no anexe contenido al archivo `~/instance_output`.

- 6.1. Detenga el proceso `instance network`. Verifique que el proceso esté detenido.

```
[student@servera bin]$ kill -SIGSTOP %1
[1]+ Stopped           instance network
[student@servera bin]$ jobs
[1]+ Stopped           instance network
[2]  Running           instance interface &
[3]- Running           instance connection &
```

- 6.2. En la shell de terminal derecha, vea la salida del comando `tail`. Confirme que la palabra `network` ya no esté anexada al archivo `~/instance_outfile`.

```
...output omitted...
interface connection interface connection interface connection interface
```

- 7. En la shell de terminal izquierda, finalice el proceso `instance interface`. Verifique que el proceso `instance interface` haya desaparecido. Confirme que la salida del proceso `instance interface` ya no esté anexada al archivo `~/instance_outfile`.

- 7.1. Finalice el proceso `instance interface`. Verifique que el proceso haya terminado.

```
[student@servera bin]$ kill -SIGTERM %2
[student@servera bin]$ jobs
[1]+  Stopped                  instance network
[2]-  Terminated                instance interface
[3]-  Running                   instance connection &
```

- 7.2. En la shell de terminal derecha, vea la salida del comando `tail`. Confirme que la palabra `interface` ya no esté anexada al archivo `~/instance_outfile`.

```
...output omitted...
connection connection connection connection connection connection connection
connection
```

- 8. En la shell de terminal izquierda, reanude el proceso `instance network`. Verifique que el proceso `instance network` esté configurado como `Running`. Confirme que la salida del proceso `instance network` no esté anexada al archivo `~/instance_outfile`.

- 8.1. Reanude el proceso `instance network`. Compruebe que el proceso tenga el estado `Running`.

```
[student@servera bin]$ kill -SIGCONT %1
[student@servera bin]$ jobs
[1]+  Running                   instance network &
[3]-  Running                   instance connection &
```

- 8.2. En la shell de terminal derecha, vea la salida del comando `tail`. Verifique que la palabra `network` esté anexada al archivo `~/instance_outfile`.

```
...output omitted...
network connection network connection network connection network connection
network connection
```

- 9. En la shell de terminal izquierda, finalice los dos trabajos restantes. Verifique que no queden trabajos y que se haya detenido la salida.

- 9.1. Finalice el proceso `instance network`. A continuación, finalice el proceso `instance connection`.

```
[student@servera bin]$ kill -SIGTERM %1
[student@servera bin]$ kill -SIGTERM %3
[1]+ Terminated instance network
[student@servera bin]$ jobs
[3]+ Terminated instance connection
```

- 10. En la shell de terminal izquierda, enumere los procesos que se están ejecutando en todas las shells de terminales abiertas. Finalice los procesos `tail`. Verifique que los procesos ya no estén en funcionamiento.

- 10.1. Enumere todos los procesos en ejecución actuales. Refine la búsqueda para ver solo `tail` líneas.

```
[student@servera bin]$ ps -ef | grep tail
student 4581 31358 0 10:02 pts/0 00:00:00 tail -f instance_outfile
student 4869 2252 0 10:33 pts/1 00:00:00 grep --color=auto tail
```

- 10.2. Finalice el proceso `tail`. Verifique que los procesos ya no estén ejecutándose.

```
[student@servera bin]$ pkill -SIGTERM tail
[student@servera bin]$ ps -ef | grep tail
student 4874 2252 0 10:36 pts/1 00:00:00 grep --color=auto tail
```

- 10.3. En la shell de terminal derecha, verifique que el comando `tail` ya no se está ejecutando.

```
...output omitted...
network connection network connection network connection Terminated
[student@servera ~]$
```

- 11. Cierre el terminal adicional. Regrese al sistema `workstation` como el usuario `student`.

```
[student@servera bin]$ exit
logout
Connection to servera closed.
[student@workstation ~]$
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish processes-kill
```

Esto concluye la sección.

Monitoreo de la actividad de procesos

Objetivos

Definir el promedio de carga y determinar los procesos del servidor que consumen muchos recursos.

Descripción del promedio de carga

El *promedio de carga* es una medida proporcionada por el kernel de Linux para representar la carga percibida del sistema durante un periodo de tiempo. Puede usarse como un indicador aproximado de cuántas solicitudes de recursos del sistema están pendientes y para determinar si la carga del sistema aumenta o disminuye.

El kernel recoge la cantidad de carga actual cada cinco segundos en función de la cantidad de procesos en estados ejecutables e ininterrumpidos. Este número se acumula y se informa como un promedio móvil exponencial en los últimos 1, 5 y 15 minutos.

Cálculo del promedio de carga

El promedio de carga representa la carga del sistema percibida durante un período de tiempo. Linux determina la carga promedio al informar cuántos procesos están listos para ejecutarse en una CPU y cuántos procesos están esperando que se complete la E/S del disco o de la red.

- La cantidad de carga es un promedio en ejecución de la cantidad de procesos que están listos para ejecutarse (estado en proceso R) o la cantidad de procesos que están esperando a que finalice la E/S (estado en proceso D).
- Algunos sistemas UNIX solo tienen en cuenta el uso de la CPU o la longitud de la cola de ejecución para indicar la carga del sistema. Linux también incluye el uso del disco o de la red porque el uso elevado de estos recursos puede tener un impacto tan significativo en el rendimiento del sistema como la carga de la CPU. Para promedios altos de carga con actividad mínima de CPU, se debe examinar la actividad del disco y de la red.

El promedio de carga es una medida aproximada de cuántos procesos están actualmente esperando a que se complete una solicitud antes de ejecutar otra tarea. La solicitud puede ser tiempo de CPU para ejecutar el proceso. Como alternativa, la solicitud puede ser para que se complete una operación crítica de E/S del disco, y el proceso no se puede ejecutar en la CPU hasta que la solicitud se complete, incluso si la CPU está inactiva. De cualquier manera, la carga del sistema se ve afectada, y el sistema parece funcionar más lentamente porque los procesos están esperando para ejecutarse.

Interpretación de los valores del promedio de carga

El comando `uptime` es una forma de mostrar el promedio de carga actual. Imprime la hora actual, cuánto tiempo ha estado funcionando la máquina, cuántas sesiones de usuario se están ejecutando y el promedio de carga actual.

```
[user@host ~]$ uptime
15:29:03 up 14 min,  2 users,  load average: 2.92, 4.48, 5.20
```

capítulo 6 | Ajuste del rendimiento del sistema

Los tres valores del promedio de carga representan la carga durante los últimos 1, 5 y 15 minutos. Indica si la carga del sistema parece estar subiendo o bajando.

Si el promedio de carga aumenta principalmente debido a procesos que están esperando a la CPU, puede calcular el valor de carga aproximado por CPU para determinar si el sistema está experimentando una espera significativa.

Use el comando `lscpu` para determinar la cantidad de CPU presentes en un sistema.

En el siguiente ejemplo, el sistema es un sistema de un solo socket de doble núcleo con dos hyperthreads por núcleo. En términos generales, Linux tratará esta configuración de CPU como un sistema de cuatro CPU para fines de programación.

```
[user@host ~]$ lscpu
Architecture:           x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
CPU(s):                4
On-line CPU(s) list:  0-3
Thread(s) per core:   2
Core(s) per socket:   2
Socket(s):             1
NUMA node(s):          1
...output omitted...
```

Imagine por un momento que la única contribución a la cantidad de carga proviene de procesos que necesitan tiempo de CPU. Puede entonces dividir los valores promedios de carga que se muestran por el número de CPU lógicas en el sistema. Un valor por debajo de 1 indica uso de recursos adecuado y tiempos de espera mínimos. Un valor por encima de 1 indica saturación de recursos y cierto retraso en el procesamiento.

```
# From lscpu, the 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 cola de CPU inactiva tiene una cantidad de carga de 0. Cada proceso que espera a una CPU agrega un recuento de 1 a la cantidad de carga. Si un proceso se está ejecutando en una CPU, la cantidad de carga es 1, es decir, el recurso (la CPU) está en uso, pero no hay solicitudes en espera. Si ese proceso se está ejecutando durante un minuto entero, su contribución al promedio de carga de un minuto será 1.

Sin embargo, los procesos en suspensión ininterrumpida para E/S críticas debido a un disco o recurso de red ocupados se incluyen también en el recuento y aumentan el promedio de carga. Si bien no es una indicación del uso de la CPU, estos procesos se agregan al recuento de la cola porque están esperando recursos y no pueden ejecutarse en una CPU hasta que obtienen esos recursos. Esta métrica sigue siendo una carga del sistema debido a las limitaciones de recursos que están haciendo que los procesos no se ejecuten.

Hasta que no se produce una saturación del recurso, un promedio de carga se mantiene por debajo de 1, dado que las tareas rara vez son encontradas en las colas 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 el uso 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 comando `top` es una vista dinámica de los procesos del sistema, que muestra un encabezado del resumen seguido de un proceso o lista de hilos. A diferencia del resultado estático del comando `ps`, el comando `top` continuamente se actualiza a un intervalo configurable y ofrece capacidades de reorganización, ordenado y resaltado de columnas. Puede realizar cambios persistentes en la configuración de `top`. Las columnas de salida predeterminadas `top` son las siguientes:

- El ID del proceso (PID).
- El nombre de usuario (USER) es el propietario del proceso.
- La memoria virtual (VIRT) es toda la memoria que está usando el proceso, incluido el conjunto residente, las librerías compartidas y cualquier página de memoria asignada o intercambiada (etiquetado como VSZ en el comando `ps`).
- La memoria residente (RES) es la memoria física que usa el proceso, incluido cualquier objeto residente compartido (etiquetado como RSS en el comando `ps`).
- El estado del proceso (S) puede ser uno de los siguientes estados:
 - D = Suspensión ininterrumpida
 - R = En ejecución o ejecutable
 - S = En espera
 - T = Detenido o en seguimiento
 - Z = Zombie
- 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 el comando `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.
s	Cambiar la tasa de actualización (pantalla) en segundos decimales (como 0.5, 1, 5).
b	Alternar resaltado reverso para procesos Running; solo negrita de manera predeterminada.
Shift+b	Permite el uso de negrita en la visualización, en el encabezado y en los procesos <i>En ejecución</i> .

Clave	Propósito
Shift+h	Alternar subprocesos; mostrar resumen del proceso o subprocesos individuales.
u, Shift+u	Filtrar por cualquier nombre de usuario (eficaz, real).
Shift+m	Ordenar procesos enumerados por uso de memoria, en orden decreciente.
Shift+p	Ordenar procesos enumerados por uso del procesador, en orden decreciente.
k	Eliminar un proceso. Cuando recibe un aviso, ingresar PID, luego signal.
r	Ejecute el comando renice para un proceso. Cuando recibe un aviso, ingresar PID, luego nice_value.
Shift+w	Escribir (guardar) la configuración actual de lo mostrado para usarse en el próximo reinicio de top.
q	Salir.
f	Administre las columnas al habilitar o deshabilitar los campos. También puede configurar el campo de ordenamiento para top.

**nota**

Las teclas s, k y r no están disponibles cuando el comando top se inicia en un modo seguro.

**Referencias**

Páginas del manual: ps(1), top(1), uptime(1) y w(1)

► Ejercicio Guiado

Monitoreo de la actividad de procesos

En este ejercicio, usa el comando `top` para examinar dinámicamente los procesos en ejecución y controlarlos.

Resultados

- Gestionar procesos en tiempo real.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start processes-monitor
```

Instrucciones

- 1. En la máquina `workstation`, abra dos ventanas de terminal, una al lado de la otra. En esta sección, estas terminales se denominan *izquierda* y *derecha*. En cada terminal, inicie sesión en la máquina `servera` como el usuario `student`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

- 2. En la shell de terminal izquierda, cree el directorio `/home/student/bin`. Cree un script de shell denominado `monitor` en el nuevo directorio para generar una carga artificial de la CPU. Haga el archivo de script `monitor` ejecutable.

- 2.1. Cree el directorio `/home/student/bin`.

```
[student@servera ~]$ mkdir /home/student/bin
```

- 2.2. Cree el archivo de script en el directorio `/home/student/bin` con el contenido mostrado.

```
[student@servera ~]$ vim /home/student/bin/monitor
#!/bin/bash
while true; do
    var=1
    while [[ var -lt 60000 ]]; do
        var=$((var+1))
```

```
done
sleep 1
done
```

**nota**

El script **monitor** se ejecuta hasta que el proceso se termine. Genera carga artificial de CPU al realizar sesenta mil cálculos de suma. Después de generar la carga de CPU, se inactiva durante un segundo, restablece la variable y se repite.

- 2.3. Haga el archivo **monitor** ejecutable.

```
[student@servera ~]$ chmod a+x /home/student/bin/monitor
```

- ▶ 3. En la shell de terminal derecha, ejecute el comando **top**. Cambie el tamaño de la ventana para ver el contenido del comando.

```
[student@servera ~]$ top
top - 12:13:03 up 11 days, 58 min, 3 users, load average: 0.00, 0.00, 0.00
Tasks: 113 total, 2 running, 111 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.2 us, 0.0 sy, 0.0 ni, 99.8 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 1829.4 total, 1377.3 free, 193.9 used, 258.2 buff/cache
MiB Swap: 1024.0 total, 1024.0 free, 0.0 used. 1476.1 avail Mem

PID USER      PR  NI      VIRT      RES      SHR S %CPU %MEM     TIME+ COMMAND
5861 root      20   0          0          0          0 I  0.3    0.0  0:00.71 kworker/1:3-
events
6068 student   20   0  273564    4300    3688 R  0.3    0.2  0:00.01 top
  1 root      20   0  178680   13424    8924 S  0.0    0.7  0:04.03 systemd
  2 root      20   0          0          0          0 S  0.0    0.0  0:00.03 kthreadd
  3 root      0 -20          0          0          0 I  0.0    0.0  0:00.00 rcu_gp
...output omitted...
```

- ▶ 4. En la shell de terminal izquierda, determine la cantidad de CPU lógicas de esta máquina virtual.

```
[student@servera ~]$ lscpu
Architecture:           x86_64
CPU op-mode(s):         32-bit, 64-bit
Byte Order:             Little Endian
CPU(s):                 2
...output omitted...
```

- ▶ 5. En la shell de terminal izquierda, ejecute una sola instancia del archivo ejecutable **monitor** en segundo plano.

```
[student@servera ~]$ monitor &
[1] 6071
```

- ▶ 6. En la shell de terminal derecha, monitoree el comando **top**. Presione las teclas **l**, **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.

- 7. Anote la ID de proceso (PID) para el proceso **monitor**. Observe el porcentaje de CPU para el proceso, que se espera que sea alrededor del 15 % o el 25 %.

```
[student@servera ~]$ top
PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
071 student    20   0 222448  2964  2716 S 18.7  0.2   0:27.35 monitor
...output omitted...
```

Observe los promedios de carga. 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.

```
top - 12:23:45 up 11 days,  1:09,  3 users,  load average: 0.21, 0.14, 0.05
```

- 8. En la shell de terminal izquierda, ejecute una segunda instancia del archivo ejecutable **monitor** en segundo plano.

```
[student@servera ~]$ monitor &
[2] 6498
```

- 9. En la shell de terminal derecha, anote el ID de proceso (PID) para el segundo proceso de **monitor**. Observe el porcentaje de CPU para el proceso, que también se espera que sea entre el 15 % y el 25 %.

```
[student@servera ~]$ top
PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
6071 student    20   0 222448  2964  2716 S 19.0  0.2   1:36.53 monitor
6498 student    20   0 222448  2996  2748 R 15.7  0.2   0:16.34 monitor
...output omitted...
```

Observe de nuevo el promedio de carga de un minuto, que todavía es inferior a 1. Espere al menos un minuto para permitir que el cálculo se adapte a la carga de trabajo nueva.

```
top - 12:27:39 up 11 days,  1:13,  3 users,  load average: 0.36, 0.25, 0.11
```

- 10. En la shell de terminal izquierda, ejecute una tercera instancia del archivo ejecutable **monitor** en segundo plano.

```
[student@servera ~]$ monitor &
[3] 6881
```

- 11. En la shell de terminal derecha, anote el ID de proceso (PID) para el tercer proceso de **monitor**. Observe el porcentaje de CPU para el proceso, que de nuevo se espera que sea entre el 15 % y el 25 %.

```
[student@servera ~]$ top
PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
6881 student    20   0 222448  3032  2784 S 18.6  0.2  0:11.48 monitor
6498 student    20   0 222448  2996  2748 S 15.6  0.2  0:47.86 monitor
6071 student    20   0 222448  2964  2716 S 18.1  0.2  2:07.86 monitor
```

Para que el promedio de carga sea superior a 1, debe iniciar más procesos de **monitor**. La configuración del aula tiene dos CPU, por lo que solo tres procesos no son suficientes para alterarla. Inicie tres procesos **monitor** más en segundo plano. Observe de nuevo el promedio de carga de un minuto, que ahora se espera que sea superior a 1. Espere al menos un minuto para que el cálculo se adapte a la carga de trabajo nueva.

```
[student@servera ~]$ monitor &
[4] 10708
[student@servera ~]$ monitor &
[5] 11122
[student@servera ~]$ monitor &
[6] 11338
```

```
top - 12:42:32 up 11 days,  1:28,  3 users,  load average: 1.23, 2.50, 1.54
```

- 12. Una vez que haya finalizado de observar los valores promedio de carga, finalice cada uno de los procesos **monitor** desde el comando **top**.

- 12.1. En la terminal de shell derecha, presione **k** para observar el prompt que está debajo de los encabezados y arriba de las columnas.

```
...output omitted...
PID to signal/kill [default pid = 11338]
```

- 12.2. El prompt elige los procesos **monitor** en la parte superior de la lista. Presione **Enter** (**Intro**) para finalizar el proceso.

```
...output omitted...
Send pid 11338 signal [15/sigterm]
```

- 12.3. Presione **Enter** (**Intro**) de nuevo para confirmar la señal SIGTERM 15.

Verifique que el proceso seleccionado ya no esté presente en el comando **top**. Si el PID existe, repita estos pasos para finalizar los procesos y sustituya la señal SIGKILL 9 cuando se le solicite.

```
6498 student    20   0 222448  2996  2748 R 22.9  0.2  5:31.47 monitor
6881 student    20   0 222448  3032  2784 R 21.3  0.2  4:54.47 monitor
11122 student   20   0 222448  2984  2736 R 15.3  0.2  2:32.48 monitor
6071 student    20   0 222448  2964  2716 S 15.0  0.2  6:50.90 monitor
10708 student   20   0 222448  3032  2784 S 14.6  0.2  2:53.46 monitor
```

- ▶ **13.** Repita el paso anterior para cada instancia del proceso `monitor` restante. Verifique que no quede ningún proceso `monitor` en el comando `top`.
- ▶ **14.** En la shell de terminal derecha, presione `q` para salir del comando `top`. Cierre el terminal derecho.
- ▶ **15.** Regrese a la máquina `workstation` como el usuario `student`.

```
[student@servera ~]$ exit  
logout  
Connection to servera closed.  
[student@workstation ~]$
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish processes-monitor
```

Esto concluye la sección.

Ajuste de perfiles de optimización

Objetivos

Optimizar el rendimiento del sistema seleccionando un perfil de ajuste administrado por el daemon tuned.

Sistemas de ajuste

Los administradores del sistema optimizan el rendimiento de un sistema ajustando diversas configuraciones de dispositivos basadas en una variedad de cargas de trabajo de casos de uso. El daemon tuned aplica la configuración de ajuste de forma estática y dinámica, con perfiles de optimización que reflejan los requisitos particulares de la carga de trabajo.

Configuración de ajuste estático

El daemon tuned aplica la configuración del sistema cuando se inicia el servicio o al seleccionar un nuevo perfil de ajuste. El ajuste estático configura los parámetros predefinidos del kernel en los perfiles a los que se aplica el daemon tuned en el tiempo de ejecución. Con el ajuste estático, el daemon tuned define los parámetros del kernel para las expectativas de rendimiento general sin ajustar estos parámetros a medida que cambian los niveles de actividad.

Configuración de ajuste dinámico

Con el ajuste dinámico, el daemon tuned monitorea la actividad del sistema y ajusta la configuración según los cambios de comportamiento del tiempo de ejecución. El ajuste dinámico se modifica continuamente para adaptarse a la carga de trabajo actual, comenzando con los ajustes declarados iniciales en el perfil ajustado seleccionado.

Por ejemplo, los dispositivos de almacenamiento experimentan un alto uso durante el arranque y el inicio de sesión, pero tienen una actividad mínima cuando las cargas de trabajo de los usuarios consisten en el uso de navegadores web y clientes de correo electrónico. De manera similar, la actividad de la CPU y los dispositivos de red aumentan durante el uso máximo en un día laboral. El daemon tuned monitorea la actividad de estos componentes y ajusta la configuración de parámetros para maximizar el rendimiento durante momentos de mucha actividad y reducir los ajustes durante momentos de poca actividad. El daemon tuned usa los parámetros de rendimiento proporcionados en los perfiles de ajuste predefinidos.

Para monitorear y ajustar la configuración de los parámetros, el daemon tuned usa módulos denominados *complementos* (*plug-ins*) de monitoreo y ajuste, respectivamente.

Los complementos (*plug-ins*) de monitoreo analizan el sistema y obtienen información de él, de modo que los complementos (*plug-ins*) de ajuste usan esta información para el ajuste dinámico. En este momento, el daemon tuned se envía con tres complementos (*plug-ins*) de monitoreo diferentes:

- **disk**: monitorea la carga del disco en función del número de operaciones de E/S para cada dispositivo de disco.
- **net**: monitorea la carga de la red en función del número de paquetes transferidos por tarjeta de red.
- **load**: monitorea la carga de la CPU para cada CPU.

Los complementos (plug-ins) de ajuste ajustan los subsistemas individuales. Usan los datos obtenidos por los complementos (plug-ins) de monitoreo y los parámetros de rendimiento proporcionados por los perfiles de ajuste predefinidos. Entre otros, el daemon `tuned` incluye los siguientes complementos (plug-ins) de ajuste:

- `disk`: define diferentes parámetros de disco, por ejemplo, el programador de disco, el tiempo de espera de inactividad o la administración avanzada de energía.
- `net`: configura la velocidad de la interfaz y la funcionalidad Wake-on-LAN (WoL).
- `cpu`: define diferentes parámetros de CPU, por ejemplo, el regulador de CPU o la latencia.

De forma predeterminada, el ajuste dinámico está deshabilitado. Puede habilitarlo estableciendo la variable `dynamic_tuning` en 1 en el archivo de configuración `/etc/tuned/tuned-main.conf`. Si habilita el ajuste dinámico, el daemon `tuned` monitorea periódicamente el sistema y ajusta la configuración de ajuste a los cambios de comportamiento del tiempo de ejecución. Puede establecer el tiempo en segundos entre actualizaciones mediante el uso de la variable `update_interval` en el archivo de configuración `/etc/tuned/tuned-main.conf`.

```
[root@host ~]$ cat /etc/tuned/tuned-main.conf
...output omitted...
# Dynamically tune devices, if disabled only static tuning will be used.
dynamic_tuning = 1
...output omitted...
# Update interval for dynamic tunings (in seconds).
# It must be multiply of the sleep_interval.
update_interval = 10
...output omitted...
```

La utilidad de ajuste

La instalación mínima de Red Hat Enterprise Linux incluye el paquete `tuned` de manera predeterminada. Puede instalar y habilitar el paquete manualmente con los siguientes comandos:

```
[root@host ~]$ dnf install tuned
...output omitted...
[root@host ~]$ systemctl enable --now tuned
Created symlink /etc/systemd/system/multi-user.target.wants/tuned.service → /usr/
lib/systemd/system/tuned.service.
```

La aplicación `tuned` proporciona perfiles divididos en las siguientes categorías:

- Perfiles de ahorro de energía
- Perfiles de aumento de rendimiento

Los perfiles de aumento de rendimiento incluyen perfiles que se centran en los siguientes aspectos:

- Baja latencia de almacenamiento y red
- Alto rendimiento de almacenamiento y red
- Rendimiento de máquinas virtuales
- Rendimiento del host de virtualización

La siguiente tabla muestra una lista de los perfiles de ajuste distribuidos con Red Hat Enterprise Linux 9.

Perfiles de ajuste distribuidos con Red Hat Enterprise Linux 9

Perfil de ajuste	Propósito
balanced	Ideal para los sistemas que requieren un equilibrio entre ahorro de energía y rendimiento.
powersave	Ajusta el sistema para maximizar el ahorro de energía.
throughput-performance	Ajusta el sistema para maximizar el rendimiento.
accelerator-performance	Ajusta lo mismo que throughput-performance y también reduce la latencia a menos de 100 µs.
latency-performance	Ideal para los sistemas de servidores que requieren baja latencia a expensas del consumo de energía.
network-throughput	Este perfil se deriva del perfil throughput-performance. Se aplican parámetros de ajuste de red adicionales para maximizar el rendimiento de la red.
network-latency	Este perfil se deriva del perfil latency-performance. Habilita parámetros de ajuste de red adicionales para proporcionar una baja latencia de red.
desktop	Este perfil se deriva del perfil balanced. Proporciona una respuesta más rápida de las aplicaciones interactivas.
hpc-compute	Este perfil se deriva del perfil latency-performance. Ideal para computación de alto rendimiento.
virtual-guest	Ajusta el sistema para maximizar el rendimiento si se ejecuta en una máquina virtual.
virtual-host	Ajusta el sistema para maximizar el rendimiento si actúa como host de máquinas virtuales.
intel-sst	Optimizado para sistemas con configuraciones de tecnología Intel Speed Select. Úsalo como superposición en otros perfiles.
optimize-serial-console	Aumenta la capacidad de respuesta de la consola serial. Úsalo como superposición en otros perfiles.

La aplicación tuned almacena los perfiles de ajuste en los directorios /usr/lib/tuned y /etc/tuned. Cada perfil tiene un directorio separado y, dentro del directorio, el archivo de configuración principal tuned.conf y, opcionalmente, otros archivos.

```
[root@host ~]# cd /usr/lib/tuned
[root@host tuned]# ls
accelerator-performance  hpc-compute          network-throughput      throughput-
performance              balanced             intel-sst            optimize-serial-console virtual-
balanced                guest               latency-performance powersave           virtual-
guest                  desktop              network-latency       recommend.d
host                   functions             tuned.conf
[root@host tuned]$ ls virtual-guest
tuned.conf
```

Un archivo de configuración tuned.conf típico se ve de la siguiente manera:

```
[root@host tuned]# cat virtual-guest/tuned.conf
#
# tuned configuration
#

[main]
summary=Optimize for running inside a virtual guest
include=throughput-performance

[sysctl]
# If a workload mostly uses anonymous memory and it hits this limit, the entire
# working set is buffered for I/O, and any more write buffering would require
# swapping, so it's time to throttle writes until I/O can catch up. Workloads
# that mostly use file mappings may be able to use even higher values.
#
# The generator of dirty data starts writeback at this percentage (system default
# is 20%)
vm.dirty_ratio = 30

# Filesystem I/O is usually much more efficient than swapping, so try to keep
# swapping low. It's usually safe to go even lower than this on systems with
# server-grade storage.
vm.swappiness = 30
```

La sección [main] del archivo puede incluir un resumen del perfil de ajuste. Esta sección también acepta el parámetro `include`, que puede usar para hacer que el perfil herede todas las configuraciones del perfil al que se hace referencia.

Esto es muy útil al crear nuevos perfiles de ajuste, ya que puede usar uno de los perfiles provistos como base y luego agregar o modificar los parámetros que desea configurar. Para crear o modificar perfiles de ajuste, copie los archivos del perfil de ajuste del directorio `/usr/lib/tuned` al directorio `/etc/tuned` y, luego, modifíquelo. En caso de que haya directorios de perfil con el mismo nombre en los directorios `/usr/lib/tuned` y `/etc/tuned`, estos últimos siempre tienen prioridad. Nunca modifique directamente los archivos en el directorio del sistema `/usr/lib/tuned`.

El resto de las secciones del archivo `tuned.conf` usan los complementos (plug-ins) de ajuste para modificar los parámetros en el sistema. En el ejemplo anterior, la sección `[sysctl]` modifica los parámetros del kernel `vm.dirty_ratio` y `vm.swappiness` a través del complemento (plug-in) `sysctl`.

Administración de perfiles desde la línea de comandos

Use el comando `tuned-adm` para modificar la configuración del daemon `tuned`. El comando `tuned-adm` consulta la configuración actual, enumera los perfiles disponibles, recomienda un perfil de ajuste para el sistema, modifica los perfiles directamente o desactiva los ajustes.

Puede identificar el perfil de ajuste activo actualmente con el comando `tuned-adm active`.

```
[root@host ~]# tuned-adm active
Current active profile: virtual-guest
```

El comando `tuned-adm list` enumera todos los perfiles de ajuste disponibles, incluidos ambos perfiles incorporados y los perfiles de ajuste personalizados.

```
[root@host ~]# tuned-adm list
Available profiles:
- accelerator-performance      - Throughput performance based tuning with ...
- balanced                     - General non-specialized tuned profile
- desktop                      - Optimize for the desktop use-case
- hpc-compute                  - Optimize for HPC compute workloads
- intel-sst                     - Configure for Intel Speed Select Base Frequency
- latency-performance           - Optimize for deterministic performance at ...
- network-latency               - Optimize for deterministic performance at ...
...output omitted...
Current active profile: virtual-guest
```

Use el comando `tuned-adm profile profilename` para cambiar a un perfil diferente que se adapte mejor a los requisitos de ajuste actuales del sistema.

```
[root@host ~]$ tuned-adm profile throughput-performance
[root@host ~]$ tuned-adm active
Current active profile: throughput-performance
```

El comando `tuned-adm recommend` puede recomendar un perfil de ajuste para el sistema. El sistema usa este mecanismo para determinar el perfil predeterminado después de la instalación.

```
[root@host ~]$ tuned-adm recommend
virtual-guest
```



nota

El comando `tuned-adm recommend` basa su recomendación en diversas características del sistema, entre ellas, si el sistema es una máquina virtual y otras categorías predefinidas seleccionadas durante la instalación del sistema.

Para revertir los cambios de configuración que aplica el perfil actual, cambie a otro perfil o desactive el daemon ajustado. Desactive la actividad de ajuste de la aplicación `tuned` con el comando `tuned-adm off`.

```
[root@host ~]$ tuned-adm off
[root@host ~]$ tuned-adm active
No current active profile.
```

Administración de perfiles con la consola web

Para administrar los perfiles de rendimiento del sistema con la consola web, debe iniciar sesión y aumentar los privilegios. El modo de aumento de privilegios permite que el usuario ejecute comandos, con privilegios administrativos, que modifican los perfiles de rendimiento del sistema. Debido a que cambiar los perfiles de ajuste modifica algunos parámetros del sistema, debe hacerlo con privilegios administrativos.

Puede cambiar al modo de acceso administrativo en la consola web haciendo clic en los botones **Limited access** o **Turn on administrative access**. A continuación, ingrese su contraseña cuando se le solicite. Después de aumentar los privilegios, el botón **Limited access** cambia a **Administrative access**. Como recordatorio de seguridad, recuerde que siempre debe volver al modo de acceso limitado una vez que realice en su sistema la tarea que requiere privilegios administrativos.

Como usuario privilegiado, haga clic en la opción del menú **Overview** en la barra de navegación izquierda. El perfil **Performance profile** muestra el perfil activo actual.

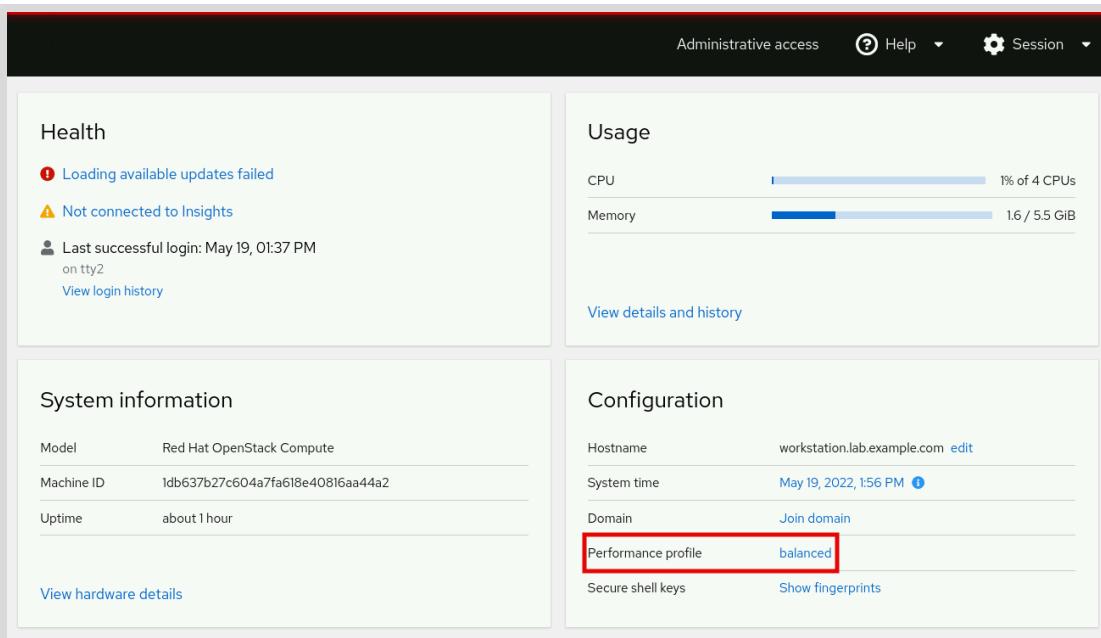


Figura 6.1: Perfil de rendimiento activo

Para seleccionar un perfil diferente, haga clic en el enlace del perfil activo. En la interfaz de usuario **Change performance profile** (Cambiar perfil de rendimiento), desplácese por la lista de perfiles para seleccionar el que mejor se adapte al propósito del sistema y haga clic en el botón **Change profile** (Cambiar perfil).

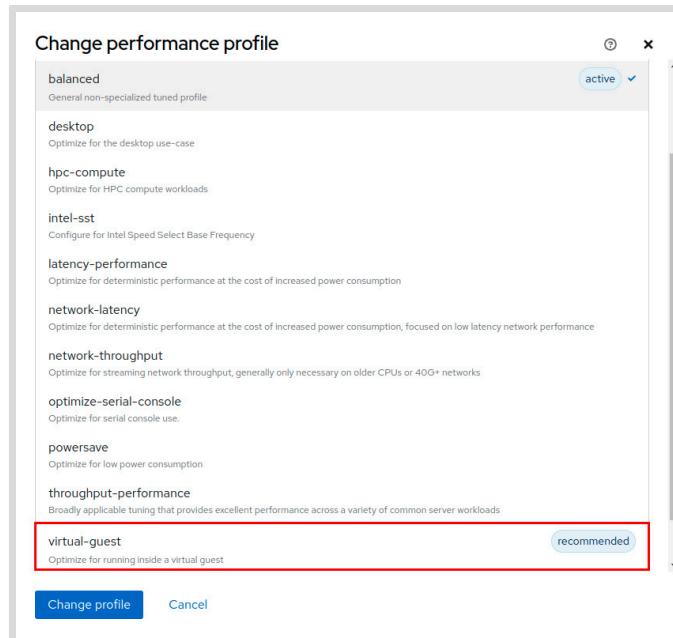


Figura 6.2: Seleccione un perfil de rendimiento preferido

Para verificar los cambios, vuelva a la página principal de **Overview** y confirme que se muestra el perfil activo en el campo **Performance profile**.



Referencias

Páginas del manual: **tuned(8)**, **tuned.conf(5)**, **tuned-main.conf(5)** y **tuned-adm(1)**

Para obtener más información, consulte la guía *Monitoring and Managing System Status and Performance* en

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/monitoring_and_managing_system_status_and_performance/index

► Ejercicio Guiado

Ajuste de perfiles de optimización

En este ejercicio, ajusta el rendimiento de un servidor activando el servicio `tuned` y aplicando un perfil de ajuste.

Resultados

- Configurar un sistema para usar un perfil de ajuste.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start tuning-profiles
```

Instrucciones

- 1. Inicie sesión en `servera` con el usuario `student`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

- 2. Verifique que el paquete `tuned` esté instalado, habilitado e iniciado.

2.1. Verifique que el paquete `tuned` esté instalado.

```
[student@servera ~]$ dnf list tuned
...output omitted...
Installed Packages
tuned.noarch           2.18.0-1.el9          @System
```

2.2. Verifique que el servicio esté habilitado.

```
[student@servera ~]$ systemctl is-enabled tuned
enabled
```

2.3. Verifique que el servicio se esté ejecutando actualmente.

```
[student@servera ~] systemctl is-active tuned
active
```

- 3. Enumere los perfiles de ajuste disponibles e identifique el perfil activo.

```
[student@servera ~]$ sudo tuned-adm list
[sudo] password for student: student
Available profiles:
- accelerator-performance      - Throughput performance based tuning with disabled
                                higher latency STOP states
- balanced                   - General non-specialized tuned profile
- desktop                     - Optimize for the desktop use-case
- hpc-compute                 - Optimize for HPC compute workloads
- intel-sst                   - Configure for Intel Speed Select Base Frequency
- latency-performance         - Optimize for deterministic performance at the cost
                                of increased power consumption
- network-latency             - Optimize for deterministic performance at the cost
                                of increased power consumption, focused on low latency network performance
- network-throughput          - Optimize for streaming network throughput,
                                generally only necessary on older CPUs or 40G+ networks
- optimize-serial-console     - Optimize for serial console use.
- powersave                  - Optimize for low power consumption
- throughput-performance      - Broadly applicable tuning that provides excellent
                                performance across a variety of common server workloads
- virtual-guest               - Optimize for running inside a virtual guest
- virtual-host                - Optimize for running KVM guests
Current active profile: virtual-guest
```

- 4. Revise el archivo de configuración `tuned.conf` para el perfil activo actual, `virtual-guest`. Puede encontrarlo en el directorio `/usr/lib/tuned/virtual-guest`. El perfil de ajuste `virtual-guest` se basa en el perfil `throughput-performance`, pero define diferentes valores para los parámetros `vm.dirty_ratio` y `vm.swappiness`. Verifique que el perfil de ajuste `virtual-guest` aplique estos valores en su sistema.
- 4.1. Revise el archivo de configuración `virtual-guest` del directorio `/usr/lib/tuned/virtual-guest`. Verifique los valores para los parámetros `vm.dirty_ratio` y `vm.swappiness`.

```
[student@servera ~]$ cat /usr/lib/tuned/virtual-guest/tuned.conf
#
# tuned configuration
#
[main]
summary=Optimize for running inside a virtual guest
include=throughput-performance

[sysctl]
# If a workload mostly uses anonymous memory and it hits this limit, the entire
# working set is buffered for I/O, and any more write buffering would require
# swapping, so it's time to throttle writes until I/O can catch up. Workloads
# that mostly use file mappings may be able to use even higher values.
#
# The generator of dirty data starts writeback at this percentage (system default
# is 20%)
vm.dirty_ratio = 30
```

capítulo 6 | Ajuste del rendimiento del sistema

```
# Filesystem I/O is usually much more efficient than swapping, so try to keep
# swapping low. It's usually safe to go even lower than this on systems with
# server-grade storage.
vm.swappiness = 30
```

4.2. Verifique que el perfil de ajuste aplique estos valores en su sistema.

```
[student@servera ~]$ sysctl vm.dirty_ratio
vm.dirty_ratio = 30
[student@servera ~]$ sysctl vm.swappiness
vm.swappiness = 30
```

- 5. Revise el archivo de configuración tuned.conf para el perfil de ajuste principal virtual-guest, throughput-performance. Puede encontrarlo en el directorio /usr/lib/tuned/throughput-performance. Observe que el perfil de ajuste throughput-performance establece un valor diferente para los parámetros vm.dirty_ratio y vm.swappiness, aunque el perfil virtual-guest los sobrescribe. Verifique que el perfil de ajuste virtual-guest aplique el valor para el parámetro vm.dirty_background_ratio, que hereda del perfil throughput-performance.
- 5.1. Revise el archivo de configuración throughput-performance del directorio /usr/lib/tuned/throughput-performance. Verifique los valores para los parámetros vm.dirty_ratio, vm.swappiness y vm.dirty_background_ratio.

```
[student@servera ~]$ cat /usr/lib/tuned/throughput-performance/tuned.conf
#
# tuned configuration
#
[main]
summary=Broadly applicable tuning that provides excellent performance across a
variety of common server workloads

...output omitted...

[sysctl]
# If a workload mostly uses anonymous memory and it hits this limit, the entire
# working set is buffered for I/O, and any more write buffering would require
# swapping, so it's time to throttle writes until I/O can catch up. Workloads
# that mostly use file mappings may be able to use even higher values.
#
# The generator of dirty data starts writeback at this percentage (system default
# is 20%)
vm.dirty_ratio = 40

# Start background writeback (via writeback threads) at this percentage (system
# default is 10%)
vm.dirty_background_ratio = 10

# PID allocation wrap value. When the kernel's next PID value
# reaches this value, it wraps back to a minimum PID value.
# PIDs of value pid_max or larger are not allocated.
#
# A suggested value for pid_max is 1024 * <# of cpu cores/threads in system>
```

capítulo 6 | Ajuste del rendimiento del sistema

```
# e.g., a box with 32 cpus, the default of 32768 is reasonable, for 64 cpus,  
# 65536, for 4096 cpus, 4194304 (which is the upper limit possible).  
#kernel.pid_max = 65536  
  
# The swappiness parameter controls the tendency of the kernel to move  
# processes out of physical memory and onto the swap disk.  
# 0 tells the kernel to avoid swapping processes out of physical memory  
# for as long as possible  
# 100 tells the kernel to aggressively swap processes out of physical memory  
# and move them to swap cache  
vm.swappiness=10  
  
...output omitted...
```

- 5.2. Verifique que el perfil de ajuste `virtual-guest` aplique el parámetro heredado `vm.dirty_background_ratio`.

```
[student@servera ~]$ sysctl vm.dirty_background_ratio  
vm.dirty_background_ratio = 10
```

- 6. Cambie el perfil de ajuste activo actual a `throughput-performance` y, a continuación, confirme los resultados. Verifique que los parámetros `vm.dirty_ratio` y `vm.swappiness` cambien a los valores en el archivo de configuración `throughput-performance`.

- 6.1. Cambie el perfil de ajuste activo actual.

```
[student@servera ~]$ sudo tuned-adm profile throughput-performance
```

- 6.2. Confirme que `throughput-performance` es el perfil de ajuste activo.

```
[student@servera ~]$ sudo tuned-adm active  
Current active profile: throughput-performance
```

- 6.3. Verifique los valores para los parámetros `vm.dirty_ratio` y `vm.swappiness`.

```
[student@servera ~]$ sysctl vm.dirty_ratio  
vm.dirty_ratio = 40  
[student@servera ~]$ sysctl vm.swappiness  
vm.swappiness = 10
```

- 7. Regrese a la máquina `workstation` como el usuario `student`.

```
[student@servera ~]$ exit  
logout  
Connection to servera closed.  
[student@workstation ~]$
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish tuning-profiles
```

Esto concluye la sección.

Influencia en la programación de procesos

Objetivos

Dar o quitar la prioridad a procesos específicos con los comandos `nice` y `renice`.

Programación de procesos de Linux

Los sistemas de cómputo modernos usan CPU de varios núcleos y subprocessos que pueden ejecutar muchos subprocessos de instrucciones simultáneamente. Las supercomputadoras de alto rendimiento más grandes pueden tener cientos o miles de CPU con cientos de núcleos de procesamiento y estructuras de subprocessos por CPU y pueden procesar millones de subprocessos de instrucciones en paralelo. Si bien un solo usuario que ejecuta muchas aplicaciones puede saturar el sistema de escritorio típico o la estación de trabajo personal con la actividad de la CPU, una estación de trabajo con el tamaño y la configuración adecuados está diseñada para adaptarse a la carga de trabajo deseada del usuario. Sin embargo, el típico servidor empresarial o de Internet gestiona cientos o miles de usuarios y solicitudes de aplicaciones por segundo, lo que puede provocar fácilmente la saturación de la CPU. Todos los sistemas bajo la carga de la CPU experimentarán escenarios que requieren el manejo de más subprocessos que las unidades de procesamiento de CPU que el sistema tiene para programar inmediatamente los subprocessos.

Linux y otros sistemas operativos usan una técnica llamada *particionamiento de tiempo* o *multitarea* para la administración de procesos. El *programador de procesos* del sistema operativo cambia rápidamente entre subprocessos en cada núcleo de CPU disponible. Este comportamiento da la impresión de que se está ejecutando una cantidad significativa de procesos al mismo tiempo.

Prioridad de los procesos

Cada proceso tiene una medida de importancia variable, conocida históricamente como una *prioridad* de proceso. Linux implementa *políticas de programación* que definen las reglas mediante las cuales se organizan y priorizan los procesos para obtener el tiempo de procesamiento de la CPU. Linux tiene diferentes *políticas de programación* diseñadas para manejar solicitudes de aplicaciones interactivas, procesamiento de aplicaciones por lotes no interactivo y requisitos de aplicaciones en tiempo real. Las políticas de programación en tiempo real aún usan prioridades de procesos y colas, pero las políticas de programación actuales que no son de tiempo real (*normales*) usan el Programador Completamente equitativo (CFS), que en su lugar organiza los procesos que esperan tiempo de CPU en un árbol de búsqueda binario. Esta introducción a la prioridad del proceso describe la política de programación predeterminada denominada `SCHED_NORMAL` o `SCHED_OTHER`.

A los procesos que se ejecutan bajo la política `SCHED_NORMAL` se les asigna una prioridad *estática* en tiempo real de 0, para garantizar que todos los procesos en tiempo real del sistema tengan una prioridad más alta que los procesos normales. Sin embargo, este valor de prioridad estática no se incluye al organizar subprocessos de procesos normales para la programación de CPU. En cambio, el algoritmo de programación CFS organiza los subprocessos de proceso normales en un árbol binario ponderado en el tiempo, con el primer ítem que tiene la menor cantidad de tiempo de CPU usado anteriormente hasta el último ítem que tiene el tiempo de CPU más acumulado.

Valor nice

El orden del árbol binario también está influenciado por un valor *nice* por proceso modifiable por el usuario, que varía de -20 (mayor prioridad) a 19 (menor prioridad), con un valor predeterminado de 0. Los procesos heredan su valor nice inicial de su proceso principal.

Un valor nice más alto indica una disminución en la prioridad del proceso con respecto al valor predeterminado, lo que puede recordarse como *hacer que el proceso sea más nice* que otros procesos. Un valor nice más bajo indica una disminución en la prioridad del proceso con respecto al valor predeterminado, lo que puede recordarse como *hacer que el proceso sea menos nice* que otros procesos.

La modificación del valor nice en un proceso aumentará o disminuirá la posición del subprocesso en el árbol binario. Aumentar el valor nice disminuirá la posición del subprocesso y disminuir el valor aumentará la posición del subprocesso.



Importante

En general, las prioridades solo determinan indirectamente la cantidad de tiempo de CPU que recibe un subprocesso de proceso. En un sistema no saturado con capacidad de CPU disponible, cada proceso se programa para el tiempo de CPU inmediato, tanto como lo deseé cada proceso. La importancia relativa del proceso, como se administra en el árbol binario, determina solo qué subprocessos se seleccionan y se colocan en las CPU primero.

En un sistema saturado de CPU, donde hay más subprocessos en espera que unidades de procesamiento de CPU, los subprocessos de mayor prioridad (menor nice) se colocan primero, hasta que todas las unidades de CPU estén ocupadas, mientras que los subprocessos de menor prioridad (mayor nice) deben esperar inicialmente en el árbol binario. Sin embargo, el Programador completamente equitativo está diseñado para balancear la importancia del proceso, los valores nice y el tiempo de CPU acumulado anterior, y ajusta dinámicamente el árbol binario de modo que todos los procesos obtengan un tiempo de CPU equitativo.

Permiso para modificar valores nice

Los usuarios con privilegios pueden disminuir el valor nice de un proceso para hacer que un proceso sea menos nice, lo que hará que un proceso se coloque repetidamente más arriba en el árbol binario y, por lo tanto, se programe con mayor frecuencia. En un sistema saturado, se reduce el tiempo total de CPU disponible para otros procesos.

Los usuarios sin privilegios solo pueden aumentar el valor nice en sus propios procesos, lo que hará que estos sean más nice y, por lo tanto, se coloquen más abajo en el árbol binario. Los usuarios sin privilegios no pueden disminuir los valores nice de sus procesos para aumentar su importancia, ni pueden ajustar los valores nice para el proceso de otro usuario.

Visualización de valores nice

Los valores nice se asignan a un valor de prioridad y ambos valores están disponibles para su visualización en los comandos de listado de procesos. Un valor nice de -20 se asigna a una prioridad 0 en el comando `top`. Un valor nice de 19 se asigna a una prioridad 39 en el comando `top`.

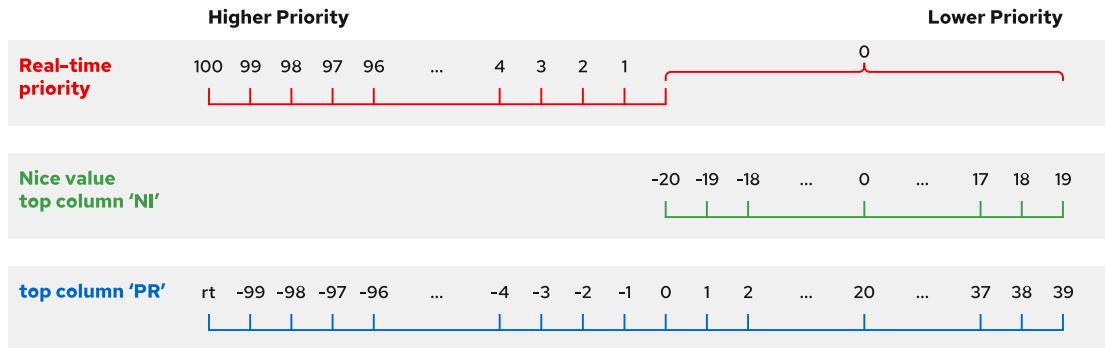


Figura 6.3: Prioridades y valores nice según lo informado por el comando top

En Figura 6.3, los valores nice se alinean con los valores de prioridad que usa el comando top. El comando top muestra la prioridad del proceso en la columna PR y el valor nice en la columna NI. El esquema de numeración de prioridad top, que muestra las prioridades del proceso en tiempo real como números negativos, se hereda de los algoritmos de prioridad internos.

La siguiente salida es el resumen y una lista parcial de procesos en el comando top:

```
Tasks: 192 total, 1 running, 191 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.0 us, 1.6 sy, 0.0 ni, 96.9 id, 0.0 wa, 0.0 hi, 1.6 si, 0.0 st
MiB Mem : 5668.6 total, 4655.6 free, 470.1 used, 542.9 buff/cache
MiB Swap: 0.0 total, 0.0 free, 0.0 used. 4942.6 avail Mem

      PID USER      PR  NI      VIRT      RES      SHR S %CPU %MEM     TIME+ COMMAND
        1 root      20   0  172180  16232  10328 S  0.0  0.3  0:01.49 systemd
        2 root      20   0          0          0      0 S  0.0  0.0  0:00.01 kthreadd
        3 root       0 -20          0          0      0 I  0.0  0.0  0:00.00 rcu_gp
        4 root       0 -20          0          0      0 I  0.0  0.0  0:00.00 rcu_par_gp
```

El comando ps muestra los valores nice del proceso cuando se usan las opciones de formato predeterminadas.

El siguiente comando ps muestra una lista de todos los procesos, con su ID del proceso, nombre del proceso, valor nice y clase de programación, ordenados de forma descendente por valor nice. En la columna de clase de programación CLS, TS significa *tiempo de uso compartido*, que es otro nombre para las políticas de programación normales, incluida SCHED_NORMAL. Otros valores CLS, como FF para *primero en entrar, primero en salir* y RR para *round robin*, indican procesos en tiempo real. A los procesos en tiempo real no se les asignan valores nice, como lo indica el guión (-) en la columna NI. Las políticas de programación avanzada se enseñan en el curso *Red Hat Performance Tuning: Linux in Physical, Virtual, and Cloud (RH442)*.

```
[user@host ~]$ ps axo pid,comm,nice,cls --sort=-nice
      PID COMMAND      NI  CLS
        33 khugepaged    19  TS
        32 ksmd         5  TS
      814 rtkit-daemon   1  TS
        1 systemd        0  TS
        2 kthreadd       0  TS
        5 kworker/0:0-cgr  0  TS
        7 kworker/0:1-rcu  0  TS
```

```
 8 kworker/u4:0-ev   0  TS
 15 migration/0      -  FF
...output omitted...
```

Iniciar procesos con valores nice definidos por el usuario

Cuando se crea un proceso, hereda el valor nice del proceso principal. Cuando un proceso se inicia desde la línea de comandos, hereda el valor nice del proceso de la shell desde donde se inició. Por lo general, los procesos nuevos se ejecutan con el valor nice predeterminado de 0.

El siguiente ejemplo inicia un proceso desde la shell y muestra el valor nice del proceso. Tenga en cuenta el uso de la opción PID en el comando ps para especificar la salida solicitada.



nota

El comando de ejemplo se usa aquí únicamente para demostrar valores nice y se eligió por su bajo consumo de recursos.

```
[user@host ~]$ sleep 60 &
[1] 2667
[user@host ~]$ ps -o pid,comm,nice 2667
  PID COMMAND      NI
 2667 sleep        0
```

Todos los usuarios pueden usar el comando nice para iniciar comandos con un valor nice predeterminado o superior. Sin opciones, el comando nice inicia un proceso con el valor nice predeterminado de 10. Definir un valor más alto de manera predeterminada garantiza que el nuevo proceso tenga una prioridad más baja que su shell de trabajo actual y es menos probable que afecte su sesión interactiva actual.

En el siguiente ejemplo, se inicia el mismo comando que una tarea en segundo plano con el valor nice predeterminado y se muestra el valor nice del proceso:

```
[user@host ~]$ nice sleep 60 &
[1] 2736
[user@host ~]$ ps -o pid,comm,nice 2736
  PID COMMAND      NI
 2736 sleep        10
```

Use la opción -n del comando nice para aplicar un valor nice definido por el usuario para el proceso de arranque. El proceso predeterminado es agregar 10 al valor nice actual del proceso. En el siguiente ejemplo, se inicia una tarea en segundo plano con el valor nice definido por el usuario de 15 y muestra el resultado:

```
[user@host ~]$ nice -n 15 sleep 60 &
[1] 2673
[user@host ~]$ ps -o pid,comm,nice 2740
  PID COMMAND      NI
 2740 sleep        15
```

**Importante**

Los usuarios sin privilegios solo pueden aumentar el valor nice de su valor actual a un máximo de 19. Una vez que aumenta el valor, los usuarios sin privilegios no pueden reducir el valor para revertir al valor nice anterior. Sin embargo, un usuario privilegiado puede reducir el valor nice de cualquier valor actual a un mínimo de -20.

Cambio del valor nice de un proceso existente

Puede cambiar el valor nice de un proceso existente con el comando `renice`. En este ejemplo, se usa el ID del proceso del ejemplo anterior para cambiar el valor nice actual de 15 a un nuevo valor nice de 19.

```
[user@host ~]$ renice -n 19 2740  
2740 (process ID) old priority 15, new priority 19
```

También puede usar el comando `top` para cambiar el valor nice en un proceso existente. Desde la interfaz interactiva `top`, presione la opción `r` para acceder al comando `renice`. Ingrese el ID del proceso y, luego, el nuevo valor nice.

**Referencias**

Páginas del manual: `nice(1)`, `renice(1)`, `top(1)` y `sched_setscheduler(2)`

► Ejercicio Guiado

Influencia en la programación de procesos

En este ejercicio, ajustará la prioridad de programación de los procesos con los comandos `nice` y `renice`, y observará los efectos en la ejecución de procesos.

Resultados

- Ajuste las prioridades de programación para los procesos.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start tuning-procscheduling
```



Importante

Este ejercicio usa comandos que realizan una suma de comprobación infinita en un archivo de dispositivo mientras usan intencionalmente recursos de CPU significativos. Verifique que haya finalizado todos los procesos del ejercicio antes de dejar este ejercicio.

Instrucciones

- 1. Use el comando `ssh` para iniciar sesión en la máquina `servera` con el usuario `student`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

- 2. Determine la cantidad de núcleos de CPU en la máquina `servera` y, a continuación, inicie dos instancias del comando `sha1sum /dev/zero &` para cada núcleo.

- 2.1. Use el comando `grep` para analizar la cantidad de procesadores virtuales existentes (núcleos de CPU) del archivo `/proc/cpuinfo`.

```
[student@servera ~]$ grep -c '^processor' /proc/cpuinfo
2
```

- 2.2. Use un comando de bucle para iniciar varias instancias del comando `sha1sum /dev/zero &`. Inicie dos instancias para cada procesador virtual que se indicó en el

capítulo 6 | Ajuste del rendimiento del sistema

paso anterior. En este ejemplo, un bucle `for` crea cuatro instancias. Los valores de PID en su salida podrían variar con respecto al ejemplo.

```
[student@servera ~]$ for i in {1..4}; do sha1sum /dev/zero & done  
[1] 1132  
[2] 1133  
[3] 1134  
[4] 1135
```

- 3. Verifique que las tareas en segundo plano se estén ejecutando para cada uno de los procesos `sha1sum`.

```
[student@servera ~]$ jobs  
[1]  Running          sha1sum /dev/zero &  
[2]  Running          sha1sum /dev/zero &  
[3]- Running          sha1sum /dev/zero &  
[4]+ Running          sha1sum /dev/zero &
```

- 4. Use los comandos `ps` y `pgrep` para mostrar el porcentaje de uso de CPU para cada proceso `sha1sum`.

```
[student@servera ~]$ ps u $(pgrep sha1sum)  
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND  
student  1132 49.6  0.1 225336  2288 pts/0    R    11:40  2:40 sha1sum /dev/zero  
student  1133 49.6  0.1 225336  2296 pts/0    R    11:40  2:40 sha1sum /dev/zero  
student  1134 49.6  0.1 225336  2264 pts/0    R    11:40  2:40 sha1sum /dev/zero  
student  1135 49.6  0.1 225336  2280 pts/0    R    11:40  2:40 sha1sum /dev/zero
```

- 5. Cierre todos los procesos `sha1sum` y, a continuación, verifique que no haya trabajos en ejecución.

- 5.1. Use el comando `kill` para cerrar todos los procesos en ejecución con el patrón de nombre `sha1sum`.

```
[student@servera ~]$ pkill sha1sum  
[2]  Terminated        sha1sum /dev/zero  
[4]+ Terminated        sha1sum /dev/zero  
[1]- Terminated        sha1sum /dev/zero  
[3]+ Terminated        sha1sum /dev/zero
```

- 5.2. Verifique que no haya trabajos en ejecución.

```
[student@servera ~]$ jobs  
[student@servera ~]$
```

- 6. Inicie varias instancias del comando `sha1sum /dev/zero &`, y, a continuación, inicie una instancia adicional del comando `sha1sum /dev/zero &` con un nivel nice de 10. Inicie tantas instancias como procesadores virtuales tenga el sistema. En este ejemplo, se inician tres instancias normales y otra con el nivel nice más alto.

- 6.1. Use los bucles para iniciar tres instancias del comando `sha1sum /dev/zero &`.

```
[student@servera ~]$ for i in {1..3}; do sha1sum /dev/zero & done
[1] 1207
[2] 1208
[3] 1209
```

- 6.2. Use el comando nice para iniciar la cuarta instancia con un nivel nice de 10.

```
[student@servera ~]$ nice -n 10 sha1sum /dev/zero &
[4] 1210
```

- 7. Use los comandos ps y pgrep para mostrar el PID, el porcentaje de uso de CPU, el valor nice y el nombre ejecutable para cada proceso. La instancia con el valor nice de 10 debe mostrar un porcentaje menor de uso de CPU que las otras instancias.

```
[student@servera ~]$ ps -o pid,pcpu,nice,comm $(pgrep sha1sum)
 PID %CPU NI COMMAND
 1207 64.2 0 sha1sum
 1208 65.0 0 sha1sum
 1209 63.9 0 sha1sum
 1210 8.2 10 sha1sum
```

- 8. Use el comando sudo renice para bajar el nivel nice de un proceso del paso anterior. Use el valor PID de la instancia del proceso con el nivel nice de 10 para reducir su nivel nice a 5.

```
[student@servera ~]$ sudo renice -n 5 1210
[sudo] password for student:
1210 (process ID) old priority 10, new priority 5
```

- 9. Repita los comandos ps y pgrep para mostrar el porcentaje de CPU y el nivel nice.

```
[student@servera ~]$ ps -o pid,pcpu,nice,comm $(pgrep sha1sum)
 PID %CPU NI COMMAND
 1207 62.9 0 sha1sum
 1208 63.2 0 sha1sum
 1209 63.2 0 sha1sum
 1210 10.9 5 sha1sum
```

- 10. Use el comando pkill para cerrar todos los procesos en ejecución con el patrón de nombre sha1sum.

```
[student@servera ~]$ pkill sha1sum
...output omitted...
```

- 11. Regrese a la máquina workstation como el usuario student.

```
[student@servera ~]$ exit  
logout  
Connection to servera closed.  
[student@workstation ~]$
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish tuning-procscheduling
```

Esto concluye la sección.

► Trabajo de laboratorio

Ajuste del rendimiento del sistema

En este trabajo de laboratorio, aplica un perfil de ajuste específico y ajustará la prioridad de programación de un proceso existente con un alto uso de CPU.

Resultados

- Activar un perfil de ajuste específico para un sistema de cómputo.
- Ajustar la prioridad de programación de CPU de un proceso.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start tuning-review
```



Importante

Este trabajo de laboratorio usa comandos que realizan una suma de comprobación infinita en un archivo de dispositivo mientras usan intencionalmente recursos de CPU significativos. Verifique que haya finalizado todos los procesos del trabajo de laboratorio antes de dejar este trabajo de laboratorio.

Instrucciones

1. Cambie el perfil de ajuste actual para la máquina `serverb` al perfil `balanced`, un perfil de ajuste general no especializado. Enumere la información para el perfil de ajuste `balanced` cuando es el perfil de ajuste actual.
2. Dos procesos en `serverb` están consumiendo un alto porcentaje de uso de CPU. Ajuste el nivel de `nice` de cada proceso en 10 para permitir más tiempo de CPU para otros procesos.

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade tuning-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish tuning-review
```

Esto concluye la sección.

► Solución

Ajuste del rendimiento del sistema

En este trabajo de laboratorio, aplica un perfil de ajuste específico y ajustará la prioridad de programación de un proceso existente con un alto uso de CPU.

Resultados

- Activar un perfil de ajuste específico para un sistema de cómputo.
- Ajustar la prioridad de programación de CPU de un proceso.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `Lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start tuning-review
```



Importante

Este trabajo de laboratorio usa comandos que realizan una suma de comprobación infinita en un archivo de dispositivo mientras usan intencionalmente recursos de CPU significativos. Verifique que haya finalizado todos los procesos del trabajo de laboratorio antes de dejar este trabajo de laboratorio.

Instrucciones

1. Cambie el perfil de ajuste actual para la máquina `serverb` al perfil `balanced`, un perfil de ajuste general no especializado. Enumere la información para el perfil de ajuste `balanced` cuando es el perfil de ajuste actual.

- 1.1. Inicie sesión en la máquina `serverb` como el usuario `student`.

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
[student@serverb ~]$
```

- 1.2. Verifique que el paquete `tuned` esté instalado.

```
[student@serverb ~]$ dnf list tuned
...output omitted...
Installed Packages
tuned.noarch           2.18.0-1.el9          @System
```

capítulo 6 | Ajuste del rendimiento del sistema

- 1.3. Verifique el estado del servicio tuned.

```
[student@serverb ~]$ systemctl is-active tuned  
active
```

- 1.4. Enumere todos los perfiles de ajuste disponibles y sus descripciones. Tenga en cuenta que el perfil activo actual es **virtual-guest**.

```
[student@serverb ~]$ sudo tuned-adm list  
[sudo] password for student: student  
Available profiles:  
- accelerator-performance      - Throughput performance based tuning with disabled  
                                higher latency STOP states  
- balanced                   - General non-specialized tuned profile  
- desktop                     - Optimize for the desktop use-case  
- hpc-compute                 - Optimize for HPC compute workloads  
- intel-sst                   - Configure for Intel Speed Select Base Frequency  
- latency-performance         - Optimize for deterministic performance at the cost  
                                of increased power consumption  
- network-latency             - Optimize for deterministic performance at the cost  
                                of increased power consumption, focused on low  
                                latency network performance  
- network-throughput          - Optimize for streaming network throughput, generally  
                                only necessary on older CPUs or 40G+ networks  
- optimize-serial-console    - Optimize for serial console use.  
- powersave                  - Optimize for low power consumption  
- throughput-performance      - Broadly applicable tuning that provides excellent  
                                performance across a variety of common server  
                                workloads  
- virtual-guest               - Optimize for running inside a virtual guest  
- virtual-host                - Optimize for running KVM guests  
Current active profile: virtual-guest
```

- 1.5. Cambie el perfil de ajuste activo actual al perfil balanced.

```
[student@serverb ~]$ sudo tuned-adm profile balanced
```

- 1.6. Enumere la información de resumen del perfil activo de ajuste actual. Verifique que el perfil **balanced** sea el perfil activo.

```
[student@serverb ~]$ sudo tuned-adm profile_info  
Profile name:  
balanced  
  
Profile summary:  
General non-specialized tuned profile  
...output omitted...
```

2. Dos procesos en **serverb** están consumiendo un alto porcentaje de uso de CPU. Ajuste el nivel de nice de cada proceso en 10 para permitir más tiempo de CPU para otros procesos.

capítulo 6 | Ajuste del rendimiento del sistema

- 2.1. Determine los dos consumidores de CPU principales en la máquina serverb. El comando ps enumera los principales consumidores de CPU en la parte inferior de la salida. Los valores de porcentaje de CPU pueden variar en su máquina.

```
[student@serverb ~]$ ps aux --sort=pcpu
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
...output omitted...
root      1079 98.5  0.1 225340  2300 ?        RN    06:25   4:29 sha1sum /dev/zero
root      1095 99.0  0.1 225340  2232 ?        R<   06:25   4:30 md5sum /dev/zero
```

- 2.2. Identifique el nivel actual de nice para los dos consumidores de CPU principales.

```
[student@serverb ~]$ ps -o pid,pcpu,nice,comm \
$(pgrep sha1sum;pgrep md5sum)
PID %CPU NI COMMAND
1079 98.8  2 sha1sum
1095 99.1 -2 md5sum
```

- 2.3. Ajuste el nivel de nice de cada proceso en 10. Use los valores de PID correctos para sus procesos de la salida del comando anterior.

```
[student@serverb ~]$ sudo renice -n 10 1079 1095
[sudo] password for student:
1079 (process ID) old priority 2, new priority 10
1095 (process ID) old priority -2, new priority 10
```

- 2.4. Verifique que el nivel actual de nice de cada proceso sea 10.

```
[student@serverb ~]$ ps -o pid,pcpu,nice,comm \
$(pgrep sha1sum;pgrep md5sum)
PID %CPU NI COMMAND
1079 98.9  10 sha1sum
1095 99.2  10 md5sum
```

- 2.5. Regrese a la máquina workstation como el usuario student.

```
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@workstation ~]$
```

Evaluación

Con el usuario student en la máquina workstation, use el comando lab para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade tuning-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish tuning-review
```

Esto concluye la sección.

Resumen

- Una señal es una interrupción de software que informa eventos a un programa en ejecución. Los comandos `kill`, `pkill` y `killall` usan señales para controlar los procesos.
- El promedio de carga es una estimación de cuán ocupado está el sistema. Para mostrar los valores promedio de carga, puede usar el comando `top`, `uptime` o `w`.
- El servicio `tuned` modifica automáticamente la configuración del dispositivo para satisfacer las necesidades específicas del sistema en función del perfil de ajuste predefinido seleccionado.
- Para revertir todos los cambios realizados en la configuración del sistema por el perfil seleccionado, cambie a otro perfil o desactive el servicio `tuned`.
- El sistema asigna una prioridad relativa a un proceso para determinar su acceso a la CPU. Esta prioridad se denomina el valor `nice` de un proceso.
- El comando `nice` asigna una prioridad a un proceso cuando se inicia.
- El comando `renice` modifica la prioridad de un proceso en ejecución.

capítulo 7

Programación de tareas futuras

Meta

Programar tareas para que se ejecuten automáticamente en el futuro

Objetivos

- Programar comandos para que se ejecuten en un horario de repetición con el archivo crontab de un usuario.
- Programar comandos para que se ejecuten en un horario de repetición con el archivo crontab y los directorios del sistema.
- Habilitar y deshabilitar los temporizadores de systemd y configurar un temporizador que administre archivos temporales

Secciones

- Programación de trabajos de usuario recurrentes (y ejercicio guiado)
- Programación de trabajos del sistema recurrentes (y ejercicio guiado)
- Administración de archivos temporales (y ejercicio guiado)

Programación de trabajos de usuario recurrentes

Objetivos

Programar comandos para que se ejecuten en un horario de repetición usando el archivo crontab de un usuario.

Descripción de trabajos de usuario recurrentes

Los trabajos recurrentes están programados para ejecutarse repetidamente. Los sistemas Red Hat Enterprise Linux proporcionan el daemon `crond`, que está habilitado e iniciado de forma predeterminada. El daemon `crond` lee múltiples archivos de configuración: uno por usuario y un conjunto de archivos en todo el sistema. Cada usuario tiene un archivo personal que edita con el comando `crontab -e`. Al ejecutar trabajos recurrentes, estos archivos de configuración proporcionan un control detallado a los usuarios y administradores. Si el trabajo programado no está escrito para usar el redireccionamiento, el daemon `crond` envía por correo electrónico cualquier salida o error generado al propietario del trabajo.

Programación de trabajos de usuario recurrentes

Use el comando `crontab` para administrar los trabajos programados. La siguiente lista muestra los comandos que puede usar un usuario local para administrar sus trabajos:

Ejemplos del comando crontab

Comando	Uso previsto
<code>crontab -l</code>	Detallar los trabajos para el usuario actual.
<code>crontab -r</code>	Eliminar todos los trabajos del usuario actual.
<code>crontab -e</code>	Editar trabajos para el usuario actual.
<code>crontab filename</code>	Eliminar todos los trabajos y reemplazar con los leídos de <i>nombre de archivo</i> . Este comando usa la entrada <code>stdin</code> cuando no se especifica ningún archivo.

Un usuario con privilegios puede usar la opción `-u` del comando `crontab` para administrar trabajos para otro usuario. El comando `crontab` nunca se usa para administrar trabajos del sistema y no se recomienda usar los comandos `crontab` como el usuario `root` debido a la capacidad de explotar trabajos personales configurados para ejecutarse como `root`. Dichos trabajos privilegiados deben configurarse como se describe en la sección posterior que describe los trabajos recurrentes del sistema.

Descripción del formato de trabajo del usuario

El comando `crontab -e` invoca el editor `vim` de manera predeterminada, a menos que la variable de entorno `EDITOR` esté configurada para otro editor. Cada trabajo debe usar una línea única en el archivo `crontab`. Siga estas recomendaciones para entradas válidas al escribir trabajos recurrentes:

- Líneas vacías para facilitar la lectura.
- Comentarios sobre las líneas que comienzan con el signo de número (#).
- Variables de entorno con formato NAME=value, que afectan a todas las líneas después de la línea donde se declaran.

La configuración de las variables estándares incluye la variable **SHELL** para declarar la shell que se usa para interpretar las líneas restantes del archivo **crontab**. La variable **MAILTO** determina quién debe recibir la salida enviada por correo electrónico.



nota

La capacidad de enviar un correo electrónico requiere una configuración adicional del sistema para un servidor de correo local o un retransmisor SMTP.

Los campos en el archivo **crontab** aparecen en el siguiente orden:

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

El comando se ejecuta cuando los campos *Day of the month* (Día del mes) o *Day of the week* (Día de la semana) usan el mismo valor que no sea el carácter *. Por ejemplo, para ejecutar un comando el día 11 de cada mes y todos los viernes a las 12:15 (formato de 24 horas), use el siguiente formato de trabajo:

```
15 12 11 * Fri command
```

Los primeros cinco campos usan las mismas reglas de sintaxis:

- Use el carácter * para ejecutar en todas las instancias posibles del campo.
- Un número para especificar la cantidad de minutos u horas, una fecha o un día de la semana. Para los días de semana, 0 equivale a domingo, 1 equivale a lunes, 2 equivale a martes, etc. 7 también equivale a domingo.
- Use x - y para un rango, que incluye los valores x y y.
- Use x, y para listas. Las listas también pueden incluir rangos, por ejemplo, 5, 10-13, 17 en la columna Minutes, para indicar que un trabajo debe ejecutarse a los 5 minutos, a los 10 minutos, a los 11 minutos, a los 12 minutos, a los 13 minutos y a los 17 minutos de la hora.
- */x indica un intervalo de x, por ejemplo, */7 en la columna Minutes ejecuta un trabajo exactamente cada siete minutos.

Asimismo, se usan abreviaturas en inglés de tres letras para los meses o los días de la semana, por ejemplo, Jan (enero), Feb (febrero) y Mon (lunes), Tue (martes).

El último campo contiene el comando completo con opciones y argumentos que se ejecutará usando la shell predeterminada. Si el comando contiene un símbolo de porcentaje no codificado (%), ese símbolo de porcentaje se tratará como el carácter de una línea nueva, y todo lo que esté después del símbolo de porcentaje se enviará al comando como enterada **stdin**.

Ejemplos de trabajos de usuario recurrentes

El siguiente trabajo ejecuta el comando `/usr/local/bin/yearly_backup` exactamente a las 9:00 a. m. el 3 de febrero, todos los años. Febrero se representa como el número 2 en el ejemplo, ya que es el segundo mes del año.

```
0 9 3 2 * /usr/local/bin/yearly_backup
```

El siguiente trabajo envía un correo electrónico que contiene la palabra **Chime** al propietario de este trabajo, cada cinco minutos entre las 9:00 a. m. y las 4:00 p. m., pero solo en cada viernes de julio.

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

El rango de horas 9-16 precedente significa que el temporizador de trabajo comienza a la novena hora (09:00) y continúa hasta el final de la decimosexta hora (16:59). El trabajo comienza a ejecutarse a las 09 : 00 con la última ejecución a las 16 : 55 porque a cinco minutos de las 16 : 55 es 17 : 00 que está más allá del alcance de las horas dadas.

Si un rango es específico para las horas en lugar de un valor único, todas las horas dentro del rango coincidirán. Por lo tanto, con las horas de 9-16, este ejemplo coincide cada cinco minutos desde las 09:00 hasta las 16:55.



nota

Este trabajo de ejemplo envía la salida como un correo electrónico porque `crond` reconoce que el trabajo permitió que la salida fuera al canal `STDIO` sin redirección. Dado que los trabajos cron se ejecutan en un entorno en segundo plano sin un dispositivo de salida (conocido como *terminal de control*), `crond` almacena en búfer la salida y crea un correo electrónico para enviarlo al usuario especificado en la configuración. Para los trabajos del sistema, el correo electrónico se enviará a la cuenta `root`.

El siguiente trabajo ejecuta el comando `/usr/local/bin/daily_report` todos los días hábiles (de lunes a viernes) dos minutos antes de la medianoche.

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

El siguiente trabajo ejecuta el comando `mutt` para enviar el mensaje de correo **Checking in** al destinatario `developer@example.com` en cada día de trabajo (lunes a viernes), a las 9:00 a. m.

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



Referencias

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

► Ejercicio Guiado

Programación de trabajos de usuario recurrentes

En este ejercicio, programará comandos para ejecutar en un programa de repetición como un usuario no privilegiado con el comando `crontab`.

Resultados

- Programar trabajos recurrentes para ejecutar como usuario no privilegiado.
- Inspeccionar los comandos que ejecuta un trabajo recurrente programado.
- Eliminar trabajos recurrentes programados.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start scheduling-cron
```

Instrucciones

- 1. Inicie sesión en la máquina `servera` como el usuario `student`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

- 2. Programe un trabajo recurrente como el usuario `student` que anexa la fecha y hora actuales al archivo `/home/student/my_first_cron_job.txt` cada dos minutos. El trabajo debe ejecutarse solo de lunes a viernes, no los sábados ni los domingos.



Importante

Si está trabajando en este ejercicio fuera de los días especificados en la instrucción anterior, ajuste la hora o la fecha del sistema en consecuencia para que el trabajo se ejecute mientras está trabajando.

- 2.1. Abra el archivo `crontab` con el editor de textos predeterminado.

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

- 2.2. Inserte la siguiente línea:

```
* /2 * * * Mon-Fri /usr/bin/date >> /home/student/my_first_cron_job.txt
```

- 2.3. Presione Esc y escriba :wq para guardar los cambios y salir del editor. Cuando el editor sale, debe ver la siguiente salida:

```
...output omitted...
crontab: installing new crontab
[student@servera ~]$
```

- 3. Use el comando **crontab -l** para enumerar los trabajos recurrentes programados. Inspeccione el comando que programó para que se ejecute como un trabajo recurrente en el paso anterior. Verifique que el trabajo ejecute el comando `/usr/bin/date` y anexe su salida al archivo `/home/student/my_first_cron_job.txt`.

```
[student@servera ~]$ crontab -l
* /2 * * * Mon-Fri /usr/bin/date >> /home/student/my_first_cron_job.txt
```

- 4. Coloque su prompt de shell en espera hasta que se cree el archivo `/home/student/my_first_cron_job.txt` como resultado de la ejecución exitosa del trabajo recurrente que programó. Espere a que regrese su prompt de shell. El comando `while ! test -f` para continuar ejecutando un bucle y está en reposo por un segundo hasta que se crea el archivo `my_first_cron_job.txt` en el directorio `/home/student`.

```
[student@servera ~]$ while ! test -f my_first_cron_job.txt; do sleep 1s; done
```

- 5. Verifique que el contenido de `/home/student/my_first_cron_job.txt` coincida con la salida del comando `date`.

```
[student@servera ~]$ cat my_first_cron_job.txt
Mon Apr  4 03:04:01 AM EDT 2022
```

- 6. Elimine todos los trabajos recurrentes programados para el usuario `student`.

- 6.1. Elimine todos los trabajos recurrentes programados para el usuario `student`.

```
[student@servera ~]$ crontab -r
```

- 6.2. Verifique que no existen trabajos recurrentes para el usuario `student`.

```
[student@servera ~]$ crontab -l
no crontab for student
```

- 6.3. Regrese a la máquina `workstation` como el usuario `student`.

```
[student@servera ~]$ exit  
logout  
Connection to servera closed.  
[student@workstation ~]$
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish scheduling-cron
```

Esto concluye la sección.

Programación de trabajos del sistema recurrentes

Objetivos

Programar comandos para que se ejecuten en un horario de repetición con el archivo crontab del sistema y directorios.

Trabajos del sistema recurrentes

Los administradores de sistemas a menudo necesitan ejecutar trabajos recurrentes. Lo mejor es ejecutar estos trabajos desde cuentas del sistema en lugar de desde cuentas de usuario. Programe estos trabajos con archivos crontab de todo el sistema en lugar de con el comando crontab. Las entradas de trabajo en los archivos crontab de todo el sistema son similares a las entradas crontab de los usuarios. Los archivos crontab de todo el sistema tienen un campo adicional antes del campo command para especificar el usuario que ejecuta el comando.

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

```

SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root

# 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

```

El archivo /etc/crontab y otros archivos en el directorio /etc/cron.d/ definen los trabajos recurrentes del sistema. Siempre debe crear sus archivos crontab personalizados en el directorio /etc/cron.d/ para programar trabajos recurrentes del sistema. Coloque el archivo crontab personalizado en el directorio /etc/cron.d para evitar que una actualización de paquete sobrescriba el archivo /etc/crontab. Los paquetes que requieren trabajos recurrentes del sistema colocan sus archivos crontab en el directorio /etc/cron.d/ que contiene las entradas de trabajo. Los administradores también usan esta ubicación para agrupar trabajos relacionados en un solo archivo.

El sistema crontab también incluye repositorios para scripts para ejecutarse cada hora, día, semana y mes. Estos repositorios están ubicados en los directorios /etc/cron.hourly/, /etc/cron.daily/, /etc/cron.weekly/ y /etc/cron.monthly/. Estos directorios contienen scripts de shell ejecutables, no archivos crontab.

**nota**

Use el comando `chmod +x script_name` para hacer un script ejecutable. Si un script no es ejecutable, no se ejecuta.

Ejecución de comandos periódicos con Anacron

El comando `run-parts` también ejecuta los trabajos diarios, semanales y mensuales desde el archivo de configuración `/etc/anacrontab`.

El archivo `/etc/anacrontab` garantiza que los trabajos programados se ejecuten siempre y que no se omitan accidentalmente porque el sistema se apagó o se hibernó. Por ejemplo, si un trabajo del sistema que se ejecuta diariamente no se ejecutó en un momento específico debido a que el sistema se estaba reiniciando, el trabajo se completa cuando el sistema está listo. Puede ocurrir un retraso antes de que se inicie el trabajo, si se especifica en el parámetro `Delay in minutes` en el archivo `/etc/anacrontab`.

Los archivos en el directorio `/var/spool/anacron/` determinan los trabajos diarios, semanales y mensuales. Cuando el daemon `crond` comienza un trabajo desde `/etc/anacrontab`, actualiza los sellos de hora de esos archivos. Con este sello de hora, puede determinar la última vez que se ejecutó el trabajo. La sintaxis del archivo `/etc/anacrontab` es diferente a la de los archivos de configuración de `crontab` regulares. El archivo `/etc/anacrontab` contiene cuatro campos por línea, como se detalla a continuación.

Period in days

Define el intervalo en días para el trabajo que se ejecuta en una programación recurrente. Este campo acepta un valor entero o macro. Por ejemplo, la macro `@daily` es equivalente al entero 1, lo que ejecuta el trabajo diariamente. De manera similar, la macro `@weekly` es equivalente al entero 7, lo que ejecuta el trabajo semanalmente.

Delay in minutes

Define el tiempo que el daemon `crond` debe esperar antes de iniciar el trabajo.

Job identifier

Este campo identifica el nombre único del trabajo en los mensajes de registro.

Command

El comando que se ejecutará.

El archivo `/etc/anacrontab` también contiene declaraciones variables del entorno con la sintaxis `NAME=value`. La variable `START_HOURS_RANGE` especifica el intervalo de tiempo para que se ejecuten los trabajos. Los trabajos no se inician fuera de este rango. Cuando un trabajo no se ejecuta dentro de este intervalo de tiempo en un día particular, el trabajo tiene que esperar hasta el día siguiente para su ejecución.

Temporizador systemd

La unidad de temporizador `systemd` activa otra unidad de un tipo diferente (como un servicio) cuyo nombre de unidad coincide con el nombre de la unidad del temporizador. La unidad del temporizador permite la activación basada en el temporizador de otras unidades. El temporizador `systemd` registra los eventos del temporizador en los diarios (journals) del sistema para una depuración más fácil.

Unidad de temporizador de muestra

El paquete sysstat proporciona la unidad de temporizador `systemd`, llamada el servicio `sysstat-collect.timer`, para recopilar estadísticas del sistema cada 10 minutos. En la siguiente salida, se muestra el contenido del archivo de configuración `/usr/lib/systemd/system/sysstat-collect.timer`.

```
...output omitted...
[Unit]
Description=Run system activity accounting tool every 10 minutes

[Timer]
OnCalendar=*:00/10

[Install]
WantedBy=sysstat.service
```

La opción `OnCalendar=*:00/10` significa que esta unidad de temporizador activa la unidad `sysstat-collect.service` correspondiente cada 10 minutos. Puede especificar intervalos de tiempo más complejos.

Por ejemplo, un valor de `2022-04-* 12:35,37,39:16` frente a la opción `OnCalendar` hace que la unidad del temporizador active la unidad de servicio correspondiente a la hora `12:35:16, 12:37:16` y `12:39:16`, todos los días durante abril de 2022. También puede especificar temporizadores relativos con la opción `OnUnitActiveSec`. Por ejemplo, con la opción `OnUnitActiveSec=15min`, la unidad del temporizador desencadena la unidad correspondiente 15 minutos después de la última vez que la unidad del temporizador activó su unidad correspondiente.



Importante

No modifique ninguna unidad en los archivos de configuración bajo el directorio `/usr/lib/systemd/system` porque la unidad `systemd` anula los cambios de configuración que realizó en ese archivo. Cree una copia del archivo de configuración en el directorio `/etc/systemd/system` y, luego, modifique el archivo copiado para evitar que cualquier actualización del paquete proveedor anule los cambios. Si existen dos archivos con el mismo nombre bajo los directorios `/usr/lib/systemd/system` y `/etc/systemd/system`, la unidad del temporizador `systemd` analiza el archivo bajo el directorio `/etc/systemd/system`.

Después de cambiar el archivo de configuración de la unidad del temporizador, use el comando `systemctl daemon-reload` para asegurar que la unidad del temporizador `systemd` cargue los cambios.

```
[root@host ~]# systemctl daemon-reload
```

Después de recargar la configuración del daemon `systemd`, use el comando `systemctl` para activar la unidad del temporizador.

```
[root@host ~]# systemctl enable --now <unitname>.timer
```



Referencias

Páginas del manual `crontab(5)`,`anacron(8)`,`anacrontab(5)`, `systemd.time(7)`,
`systemd.timer(5)` y `crond(8)`

► Ejercicio Guiado

Programación de trabajos del sistema recurrentes

En este ejercicio, programa comandos para que se ejecuten en diversos horarios agregando archivos de configuración a los directorios crontab del sistema.

Resultados

- Programar un trabajo del sistema recurrente para contar el número de usuarios activos
- Actualizar la unidad de temporizador `systemd` que recopila los datos de actividad del sistema.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start scheduling-system
```

Instrucciones

- 1. Inicie sesión en la máquina `servera` como el usuario `student` y cambie al usuario `root`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

- 2. Programe un trabajo del sistema recurrente que genere un mensaje de registro que indique la cantidad de usuarios activos en el sistema. Este trabajo debe ejecutarse diariamente y usar el comando `w -h | wc -l` para recuperar el número de usuarios activos en el sistema. Use el comando `logger` para generar el mensaje de registro de los usuarios activos actualmente.

- 2.1. Cree el archivo de script `/etc/cron.daily/usercount` con el siguiente contenido:

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

- 2.2. Haga el archivo de script ejecutable.

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

- 3. Instale el paquete sysstat. La unidad del temporizador debe desencadenar la unidad de servicio cada 10 minutos para recopilar datos de actividad del sistema con el script de shell /usr/lib64/sa/sa1. Modifique el archivo de configuración de la unidad del temporizador para recopilar los datos de la actividad del sistema cada dos minutos.

3.1. Instale el paquete sysstat.

```
[root@servera ~]# dnf install sysstat
...output omitted...
Is this ok [y/N]: y
...output omitted...
Complete!
```

- 3.2. Copie el archivo /usr/lib/systemd/system/sysstat-collect.timer en el archivo /etc/systemd/system/sysstat-collect.timer.

```
[root@servera ~]# cp /usr/lib/systemd/system/sysstat-collect.timer \
/etc/systemd/system/sysstat-collect.timer
```

- 3.3. Edite el archivo /etc/systemd/system/sysstat-collect.timer para que la unidad del temporizador funcione cada dos minutos. Reemplace todas las apariciones de la cadena 10 minutes con 2 minutes en todo el archivo de configuración de la unidad, incluidas las apariciones de las líneas comentadas. Use el comando vim /etc/systemd/system/sysstat-collect.timer para editar el archivo de configuración.

A partir de estos cambios, la unidad sysstat-collect.timer desencadena la unidad sysstat-collect.service cada dos minutos y recopila los datos de actividad del sistema en un archivo binario en el directorio /var/log/sa.

```
...output omitted...
# Activates activity collector every 2 minutes

[Unit]
Description=Run system activity accounting tool every 2 minutes

[Timer]
OnCalendar=*:00/2

[Install]
WantedBy=sysstat.service
```

- 3.4. Haga que el daemon systemd conozca los cambios.

```
[root@servera ~]# systemctl daemon-reload
```

- 3.5. Active la unidad sysstat-collect.timer.

```
[root@servera ~]# systemctl enable --now sysstat-collect.timer
...output omitted...
```

- 3.6. Espere hasta que se cree el archivo binario en el directorio /var/log/sa.

El comando `while`, `ls /var/log/sa | wc -l` devuelve 0 cuando el archivo no existe, o devuelve 1 cuando el archivo existe. El comando `while` se detiene durante un segundo cuando el archivo no está presente. El bucle `while` sale cuando el archivo está presente.

```
[root@servera ~]# while [ $(ls /var/log/sa | wc -l) -eq 0 ]; \
do sleep 1s; done
```

- 3.7. Verifique que el archivo binario en el directorio /var/log/sa se haya modificado en los últimos dos minutos.

```
[root@servera ~]# ls -l /var/log/sa
total 4
-rw-r--r--. 1 root root 2540 Apr  5 04:08 sa05
[root@servera ~]# date
Tue Apr  5 04:08:29 AM EDT 2022
```

- 3.8. Regrese a la máquina `workstation` como el usuario `student`.

```
[root@servera ~]# exit
logout
[student@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish scheduling-system
```

Esto concluye la sección.

Administración de archivos temporales

Objetivos

Habilitar y deshabilitar los temporizadores de `systemd` y configurar un temporizador que administre archivos temporales.

Administración de archivos temporales

La mayoría de las aplicaciones y servicios críticos usan archivos y directorios temporales. Algunas aplicaciones (y usuarios) usan el directorio `/tmp` para almacenar datos de trabajo transitorios, mientras que otras aplicaciones usan ubicaciones específicas de la tarea como directorios volátiles `daemon` y específicos del usuario en `/run`, que existe solo en la memoria. Cuando el sistema se reinicia o pierde energía, los sistemas de archivos basados en memoria se limpian automáticamente.

Por lo general, los daemons y los scripts funcionan correctamente solo cuando existen los archivos y directorios temporales esperados. Además, es necesario purgar los archivos temporales ubicados en el almacenamiento persistente para evitar problemas de espacio en disco o datos de trabajo obsoletos.

Red Hat Enterprise Linux incluye la herramienta `systemd-tmpfiles`, que proporciona un método estructurado y configurable para administrar directorios y archivos temporales.

En el arranque del sistema, una de las primeras unidades de servicio `systemd` lanzadas es el servicio `systemd-tmpfiles-setup`. Este servicio ejecuta las opciones `--create` `--remove` del comando `systemd-tmpfiles`, que lee las instrucciones de los archivos de configuración `/usr/lib/tmpfiles.d/*.conf`, `/run/tmpfiles.d/*.conf` y `/etc/tmpfiles.d/*.conf`. Estos archivos de configuración enumeran los archivos y directorios que el servicio `systemd-tmpfiles-setup` debe crear, eliminar o proteger con permisos.

Limpieza de archivos temporales con un temporizador de `systemd`

Para evitar que los sistemas de larga duración llenen sus discos con datos obsoletos, una unidad de temporizador `systemd` denominada `systemd-tmpfiles-clean.timer` desencadena `systemd-tmpfiles-clean.service` en un intervalo regular, que ejecuta el comando `systemd-tmpfiles --clean`.

La configuración de una unidad de temporizador `systemd` tiene una sección `[Timer]` para indicar cómo iniciar el servicio con el mismo nombre que el temporizador.

Use el siguiente comando `systemctl` para ver el contenido del archivo de configuración de la unidad `systemd-tmpfiles-clean.timer`.

```
[user@host ~]$ systemctl cat systemd-tmpfiles-clean.timer
# /usr/lib/systemd/system/systemd-tmpfiles-clean.timer
# SPDX-License-Identifier: LGPL-2.1-or-later
#
# This file is part of systemd.
#
```

```
# systemd is free software; you can redistribute it and/or modify it
# under the terms of the GNU Lesser General Public License as published by
# the Free Software Foundation; either version 2.1 of the License, or
# (at your option) any later version.

[Unit]
Description=Daily Cleanup of Temporary Directories
Documentation=man:tmpfiles.d(5) man:systemd-tmpfiles(8)
ConditionPathExists=!/etc/initrd-release

[Timer]
OnBootSec=15min
OnUnitActiveSec=1d
```

En la configuración anterior, el parámetro `OnBootSec=15min` indica que la unidad `systemd-tmpfiles-clean.service` se desencadena 15 minutos después de que el sistema se haya iniciado. El parámetro `OnUnitActiveSec=1d` indica que cualquier otro desencadenador para la unidad `systemd-tmpfiles-clean.service` ocurre 24 horas después de que la unidad de servicio se activó por última vez.

Cambie los parámetros en el archivo de configuración de la unidad del temporizador `systemd-tmpfiles-clean.timer`. Por ejemplo, un valor `30min` para el parámetro `OnUnitActiveSec` desencadena la unidad de servicio `systemd-tmpfiles-clean.service` 30 minutos después de la última activación de la unidad de servicio. Como resultado, `systemd-tmpfiles-clean.service` se activa cada 30 minutos después de que se reconozcan los cambios.

Después de cambiar el archivo de configuración de la unidad del temporizador, use el comando `systemctl daemon-reload` para asegurar que `systemd` cargue la nueva configuración.

```
[root@host ~]# systemctl daemon-reload
```

Después de recargar la configuración del administrador `systemd`, use el siguiente comando `systemctl` para activar la unidad `systemd-tmpfiles-clean.timer`.

```
[root@host ~]# systemctl enable --now systemd-tmpfiles-clean.timer
```

Limpieza manual de archivos temporales

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

Encuentre información detallada acerca del formato de los archivos de configuración para el servicio `systemd-tmpfiles` en la página del manual `tmpfiles.d(5)`. La sintaxis básica consta de las siguientes columnas: Tipo, Ruta, Modo, UID, GID, Edad y Argumento. Tipo se refiere a la acción que el servicio `systemd-tmpfiles` debe realizar; por ejemplo, `d` para crear un directorio si aún no existe o `Z` para restaurar recursivamente contextos de SELinux, permisos de archivos y propiedad.

A continuación, se dan ejemplos de configuración de purgación con explicaciones:

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

Al crear archivos y directorios, cree el directorio `/run/systemd/seats` si no existe, con el usuario `root` y el grupo de propietarios `root`, y con permisos de `rwxr-xr-x`. Si este directorio existe, no realice ninguna acción. El servicio `systemd-tmpfiles` no purga este directorio automáticamente.

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

Cree el directorio `/home/student` si aún no existe. Si existe, vacíe todo su contenido. Cuando el sistema ejecuta el comando `systemd-tmpfiles --clean`, elimina todos los archivos en el directorio a los que no accedió, que no cambió ni modificó durante más de un día.

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

Cree el enlace simbólico `/run/fstablink` para apuntar a la carpeta `/etc/fstab`. Nunca purge automáticamente esta línea.

Precedencia de archivos de configuración

Los archivos de configuración `systemd-tmpfiles-clean` pueden encontrarse en tres lugares:

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

Use los archivos en el directorio `/etc/tmpfiles.d/` para configurar ubicaciones temporales personalizadas y anular los valores predeterminados provistos por el proveedor. Los archivos en el directorio `/run/tmpfiles.d/` son archivos volátiles, normalmente usados por daemons para administrar sus propios archivos temporales de tiempo de ejecución. Los paquetes RPM relevantes proporcionan los archivos en el directorio `/usr/lib/tmpfiles.d/`; por lo tanto, no edite estos archivos.

Si un archivo en el directorio `/run/tmpfiles.d/` tiene el mismo nombre de archivo que un archivo en el directorio `/usr/lib/tmpfiles.d/`, el servicio usa el archivo en el directorio `/run/tmpfiles.d/`. Si un archivo en el directorio `/etc/tmpfiles.d/` tiene el mismo nombre de archivo que un archivo en el directorio `/run/tmpfiles.d/` o `/usr/lib/tmpfiles.d/`, el servicio usa el archivo en el directorio `/etc/tmpfiles.d/`.

Dadas estas reglas de precedencia, puede reemplazar fácilmente la configuración proporcionada por el proveedor si copia el archivo relevante en el directorio `/etc/tmpfiles.d/` y, luego, lo edita. Al usar estas ubicaciones de configuración correctamente, puede administrar los ajustes configurados por el administrador desde un sistema de administración de configuración central y las actualizaciones de paquetes no sobrescribirán los ajustes configurados.



nota

Cuando evalúe configuraciones nuevas o modificadas, es útil solo aplicar los comandos de un solo archivo de configuración a la vez. Especifique el nombre del archivo de configuración en la línea de comandos `systemd-tmpfiles`.



Referencias

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

► Ejercicio Guiado

Administración de archivos temporales

En este ejercicio, usted configura `systemd-tmpfiles` para cambiar la rapidez con la que elimina los archivos temporales de `/tmp`, y también para purgar periódicamente los archivos de otro directorio.

Resultados

- Configurar `systemd-tmpfiles` para eliminar archivos temporales no usados de `/tmp`.
- Configurar `systemd-tmpfiles` para purgar periódicamente archivos de otro directorio.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start scheduling-tempfiles
```

Instrucciones

- 1. Inicie sesión en el sistema `servera` como el usuario `student` y cambie al usuario `root`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

- 2. Configure el servicio `systemd-tmpfiles` para limpiar el directorio `/tmp` de los archivos no usados de los últimos cinco días. Asegúrese de que una actualización del paquete no sobrescriba los archivos de configuración.

- 2.1. Copie el archivo `/usr/lib/tmpfiles.d/tmp.conf` en el directorio `/etc/tmpfiles.d`.

```
[root@servera ~]# cp /usr/lib/tmpfiles.d/tmp.conf \
/etc/tmpfiles.d/tmp.conf
```

- 2.2. Busque la línea de configuración en el archivo `/etc/tmpfiles.d/tmp.conf` que se aplica al directorio `/tmp`. Reemplace la edad existente de los archivos temporales en esa línea de configuración con la nueva edad de 5 días. Elimine todas las otras líneas del archivo, incluidas las líneas comentadas. Puede usar el comando `vim /etc/tmpfiles.d/tmp.conf` para editar el archivo de configuración.

En la configuración, el tipo `q` es idéntico al tipo `d` e indica al servicio `systemd-tmpfiles` que cree el directorio `/tmp` si no existe. Los permisos octales del directorio deben estar establecidos en `1777`. Tanto el usuario propietario como el grupo del directorio `/tmp` deben ser `root`. El directorio `/tmp` no debe contener los archivos temporales no usados de los últimos cinco días.

El archivo `/etc/tmpfiles.d/tmp.conf` debe aparecer de la siguiente manera:

```
q /tmp 1777 root root 5d
```

- 2.3. Compruebe la configuración del archivo `/etc/tmpfiles.d/tmp.conf`.

Debido a que el comando no devuelve ningún error, confirma que los ajustes de configuración son correctos.

```
[root@servera ~]# systemctl-tmpfiles --clean /etc/tmpfiles.d/tmp.conf
```

- ▶ 3. Agregue una nueva configuración que asegure que el directorio `/run/momentary` exista con la propiedad del usuario y del grupo establecida en `root`. Los permisos octales para el directorio deben ser `0700`. La configuración debe purgar los archivos de este directorio que no se hayan usado en los últimos 30 segundos.

- 3.1. Cree el archivo `/etc/tmpfiles.d/momentary.conf` con el siguiente contenido.

Con la configuración, el servicio `systemd-tmpfiles` asegura que el directorio `/run/momentary` exista con sus permisos octales establecidos en `0700`. El propietario del directorio `/run/momentary` debe ser el usuario `root` y el grupo. El servicio purga cualquier archivo en este directorio si permanece sin usar durante 30 segundos.

```
[root@servera ~]# vim /etc/tmpfiles.d/momentary.conf
d /run/momentary 0700 root root 30s
```

- 3.2. Compruebe la configuración del archivo `/etc/tmpfiles.d/momentary.conf`. El comando crea el directorio `/run/momentary` si aún no existe.

Debido a que el comando no devuelve ningún error, confirma que los ajustes de configuración son correctos.

```
[root@servera ~]# systemctl-tmpfiles --create \
/etc/tmpfiles.d/momentary.conf
```

- 3.3. Verifique que el comando `systemd-tmpfiles` cree el directorio `/run/momentary` con los permisos, el propietario y el propietario del grupo adecuados.

El permiso octal del directorio `/run/momentary` se establece en `0700` y la propiedad del usuario y del grupo se establece en `root`.

```
[root@servera ~]# ls -ld /run/momentary
drwx----- 2 root root 40 Apr  4 06:35 /run/momentary
```

- ▶ 4. Verifique que el comando `systemd-tmpfiles --clean` elimine cualquier archivo en el directorio `/run/momentary`, no usado en los últimos 30 segundos en función de la configuración de `systemd-tmpfiles` para el directorio.

- 4.1. Cree el archivo /run/momentary/test.

```
[root@servera ~]# touch /run/momentary/test
```

- 4.2. Configure su prompt de shell para que no regrese durante 30 segundos.

```
[root@servera ~]# sleep 30
```

- 4.3. Después de que regrese el prompt de shell, limpie los archivos obsoletos del directorio /run/momentary, según la regla a la que se hace referencia en el archivo de configuración /etc/tmpfiles.d/momentary.conf.

El comando elimina el archivo /run/momentary/test, ya que permanece sin usar durante 30 segundos. Este comportamiento se basa en la regla a la que se hace referencia en el archivo de configuración /etc/tmpfiles.d/momentary.conf.

```
[root@servera ~]# systemd-tmpfiles --clean \
/etc/tmpfiles.d/momentary.conf
```

- 4.4. Verifique que el archivo /run/momentary/test no existe.

```
[root@servera ~]# ls -l /run/momentary/test
ls: cannot access '/run/momentary/test': No such file or directory
```

- 4.5. Regrese a la máquina workstation como el usuario student.

```
[root@servera ~]# exit
logout
[student@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$
```

Finalizar

En la máquina workstation, cambie al directorio de inicio de usuario student y use el comando lab para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish scheduling-tempfiles
```

Esto concluye la sección.

► Cuestionario

Programación de tareas futuras

Elija las respuestas correctas para las siguientes preguntas.

- ▶ 1. **¿Qué comando muestra todos los trabajos de usuario que programó para ejecutarse como trabajos diferidos?**
 - a. atq
 - b. atrm
 - c. at -c
 - d. at --display

- ▶ 2. **¿Qué comando elimina el trabajo de usuario diferido con el número de trabajo 5?**
 - a. at -c 5
 - b. atrm 5
 - c. at 5
 - d. at --delete 5

- ▶ 3. **¿Qué comando muestra todos los trabajos de usuario recurrentes programados para el usuario que inició sesión actualmente?**
 - a. crontab -r
 - b. crontab -l
 - c. crontab -u
 - d. crontab -v

- ▶ 4. **¿Qué formato de trabajo ejecuta /usr/local/bin/daily_backup cada hora desde las 9:00 a. m. hasta las 6:00 p. m. todos los días de lunes a viernes?**
 - a. 00 * * * Mon-Fri /usr/local/bin/daily_backup
 - b. * */9 * * Mon-Fri /usr/local/bin/daily_backup
 - c. 00 */18 * * * /usr/local/bin/daily_backup
 - d. 00 09-18 * * Mon-Fri /usr/local/bin/daily_backup

- ▶ 5. **¿Qué directorio contiene los scripts de shell destinados a ejecutarse diariamente?**
 - a. /etc/cron.d
 - b. /etc/cron.hourly
 - c. /etc/cron.daily
 - d. /etc/cron.weekly

- 6. ¿Qué archivo de configuración define la configuración de los trabajos del sistema que se ejecutan de forma diaria, semanal y mensual?
- a. /etc/crontab
 - b. /etc/anacrontab
 - c. /etc/inittab
 - d. /etc/sysconfig/crond
- 7. ¿Qué unidad systemd desencadena regularmente la limpieza de los archivos temporales?
- a. systemd-tmpfiles-clean.timer
 - b. systemd-tmpfiles-clean.service
 - c. dnf-makecache.timer
 - d. unbound-anchor.timer

► Solución

Programación de tareas futuras

Elija las respuestas correctas para las siguientes preguntas.

- ▶ 1. **¿Qué comando muestra todos los trabajos de usuario que programó para ejecutarse como trabajos diferidos?**
 - a. atq
 - b. atrm
 - c. at -c
 - d. at --display

- ▶ 2. **¿Qué comando elimina el trabajo de usuario diferido con el número de trabajo 5?**
 - a. at -c 5
 - b. atrm 5
 - c. at 5
 - d. at --delete 5

- ▶ 3. **¿Qué comando muestra todos los trabajos de usuario recurrentes programados para el usuario que inició sesión actualmente?**
 - a. crontab -r
 - b. crontab -l
 - c. crontab -u
 - d. crontab -V

- ▶ 4. **¿Qué formato de trabajo ejecuta /usr/local/bin/daily_backup cada hora desde las 9:00 a. m. hasta las 6:00 p. m. todos los días de lunes a viernes?**
 - a. 00 * * * Mon-Fri /usr/local/bin/daily_backup
 - b. * */9 * * Mon-Fri /usr/local/bin/daily_backup
 - c. 00 */18 * * * /usr/local/bin/daily_backup
 - d. 00 09-18 * * Mon-Fri /usr/local/bin/daily_backup

- ▶ 5. **¿Qué directorio contiene los scripts de shell destinados a ejecutarse diariamente?**
 - a. /etc/cron.d
 - b. /etc/cron.hourly
 - c. /etc/cron.daily
 - d. /etc/cron.weekly

- 6. ¿Qué archivo de configuración define la configuración de los trabajos del sistema que se ejecutan de forma diaria, semanal y mensual?
- a. /etc/crontab
 - b. /etc/anacrontab
 - c. /etc/inittab
 - d. /etc/sysconfig/crond
- 7. ¿Qué unidad systemd desencadena regularmente la limpieza de los archivos temporales?
- a. systemd-tmpfiles-clean.timer
 - b. systemd-tmpfiles-clean.service
 - c. dnf-makecache.timer
 - d. unbound-anchor.timer

Resumen

- Los trabajos o las tareas están programados para ejecutarse una vez en el futuro.
- Los trabajos de usuario recurrentes ejecutan las tareas del usuario en una programación de repetición.
- Los trabajos recurrentes del sistema realizan tareas administrativas en una programación de repetición que tiene impacto en todo el sistema.
- Las unidades de tipo temporizador de systemd pueden ejecutar tanto los trabajos diferidos como los recurrentes.

capítulo 8

Instalación y actualización de paquetes de software

Meta

Descargar, instalar, actualizar y gestionar paquetes de software de Red Hat y repositorios de paquetes DNF.

Objetivos

- Registrar un sistema para su cuenta de Red Hat y asignarle derechos para actualizaciones de software y servicios de soporte mediante Red Hat Suscription Management.
- Buscar, instalar y actualizar paquetes de software con el comando dnf.
- Habilitar y deshabilitar el uso de repositorios DNF de terceros o de Red Hat por un servidor.

Secciones

- Registro de sistemas para Soporte de Red Hat (y cuestionario)
- Instalación y actualización de paquetes de software con DNF (y ejercicio guiado)
- Habilitación de repositorios de software DNF (y ejercicio guiado)

Trabajo de laboratorio

- Instalación y actualización de paquetes de software

Registro de sistemas para Soporte de Red Hat

Objetivos

Registrar un sistema para su cuenta de Red Hat y asignarle derechos (entitlements) para actualizaciones de software y servicios de soporte mediante Red Hat Subscription Management.

Red Hat Subscription Management

Red Hat Subscription Management 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 estándar, como el comando `dnf`, pueden obtener paquetes y actualizaciones de software mediante una red de distribución de contenido provista por la red de entrega de contenidos de Red Hat.

Puede realizar las siguientes tareas principales con las herramientas de Red Hat Subscription Management:

- *Registrar* un sistema para asociarlo con la cuenta de Red Hat con una suscripción activa. Con el administrador de suscripciones, el sistema puede registrarse de forma única en el inventario de servicios de suscripción. Puede anular el registro del sistema cuando no esté en uso.
- *Suscribir* un sistema para autorizar las actualizaciones de productos de Red Hat seleccionados. Las suscripciones tienen niveles específicos de asistencia, fechas de vencimiento y repositorios predeterminados. Las herramientas se usan para adjuntar en forma automática o seleccionar un derecho (entitlement) específico.
- *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 deshabilitarse.
- *Revisar y rastrear* derechos (entitlements) disponibles o que se consumen. En el portal de clientes de Red Hat, puede ver la información de suscripción localmente en un sistema específico o para una cuenta de Red Hat.

Acceso a Contenido Simple

Acceso a Contenido Simple (SCA) es una función de administración de suscripciones de Red Hat. Cuando habilita SCA para su organización, el proceso de derechos (entitlements) se simplifica. SCA elimina el requisito de adjuntar suscripciones en un nivel por sistema. Usted registra sus sistemas, habilita los repositorios que cada sistema necesita y comienza a instalar paquetes de software.

Acceso a Contenido Simple es una función opcional de Red Hat Satellite Server y Red Hat Subscription Management. Este curso incluye los comandos de suscripción, según sea necesario, si aún no ha habilitado SCA.

Suscribir un sistema con la consola web de RHEL

Existen diferentes opciones para registrar un sistema en el Portal de clientes de Red Hat. Por ejemplo, puede acceder a una interfaz gráfica mediante una aplicación GNOME o mediante

la consola web de RHEL, o puede registrar su sistema mediante una herramienta de línea de comandos.

Para registrar un sistema con la consola web de RHEL, inicie la aplicación Red Hat Subscription Manager desde el menú Activities. Escriba *suscripción* en el campo Type to search y haga clic en la aplicación Red Hat Subscription Manager. Cuando se le solicite, ingrese la contraseña correspondiente para autenticarse. En la ventana Subscriptions, haga clic en Register para abrir el cuadro de diálogo Register System.

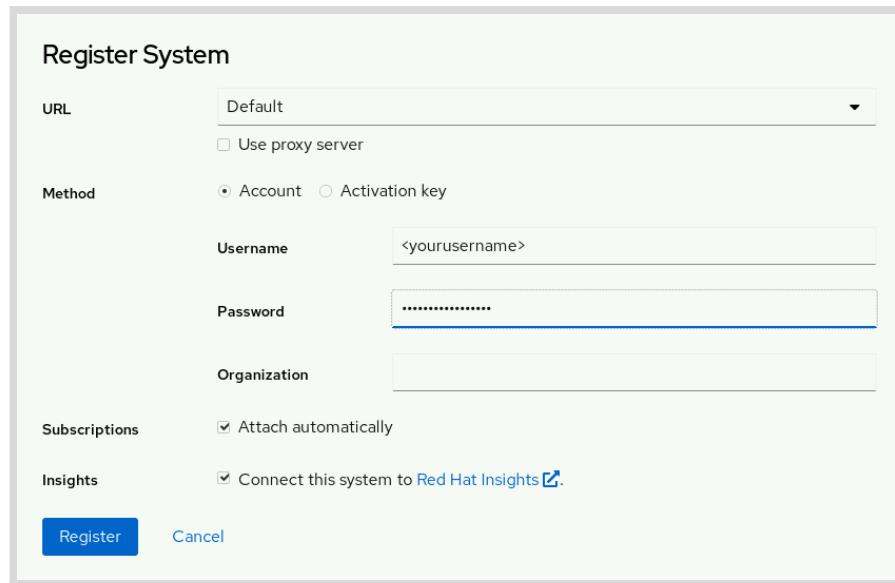


Figura 8.1: Cuadro de diálogo Registrarse en el sistema

Por defecto, los sistemas se registran en el portal del clientes de Red Hat. Proporcione el inicio de sesión y la contraseña para la cuenta del portal de clientes de Red Hat y haga clic en Register para registrarse en el sistema. Cuando está registrado, el sistema adjunta automáticamente una suscripción disponible.

Cierre la ventana Subscriptions después de registrar y asignar el sistema a una suscripción. El sistema ahora está suscrito y listo para recibir actualizaciones o instalar nuevo software de acuerdo con la suscripción que está conectada a Red Hat Content Delivery Network.

Suscribir un sistema con la línea de comandos

Use el comando subscription-manager para registrar un sistema sin usar un entorno gráfico. El comando subscription-manager adjunta automáticamente un sistema a las suscripciones compatibles que mejor coincidan para el sistema.

Registrar un sistema con las credenciales del Portal de clientes de Red Hat como usuario root :

```
[root@host ~]# subscription-manager register --username <yourusername>
Registering to: subscription.rhsm.redhat.com:443/subscription
Password: yourpassword
The system has been registered with ID: 1457f7e9-f37e-4e93-960a-c94fe08e1b4f
The registered system name is: host.example.com
```

Ver las suscripciones disponibles para su cuenta de Red Hat:

```
[root@host ~]# subscription-manager list --available
-----
 Available Subscriptions
-----
 ...output omitted...
```

Adjuntar automáticamente una suscripción:

```
[root@host ~]# subscription-manager attach --auto
...output omitted...
```

Como alternativa, adjunte una suscripción de un conjunto (pool) específico de la lista de suscripciones disponibles:

```
[root@host ~]# subscription-manager attach --pool=poolID
...output omitted...
```

Visualizar las suscripciones consumidas:

```
[root@host ~]# subscription-manager list --consumed
...output omitted...
```

Eliminar la suscripción de un sistema:

```
[root@host ~]# subscription-manager unregister
Unregistering from: subscription.rhsm.redhat.com:443/subscription
System has been unregistered.
```

Claves de activación

Una *clave de activación* es un archivo de administración de suscripciones preconfigurado que está disponible para su uso con Red Hat Satellite Server y la administración de suscripciones a través del Portal de clientes de Red Hat. Use el comando `subscription-manager` con claves de activación para simplificar el registro y la asignación de suscripciones predefinidas. Este método de registro es beneficioso para automatizar las instalaciones e implementaciones. Para las organizaciones que habilitan el Acceso Simple a Contenidos, las claves de activación pueden registrar sistemas y habilitar repositorios sin necesidad de adjuntar suscripciones.

Certificados de derechos (entitlements)

Los certificados digitales almacenan información actual sobre los derechos (entitlements) en el sistema local. El sistema registrado almacena los certificados de derechos (entitlements) en el directorio `/etc/pki`.

- Los certificados `/etc/pki/product` indican los productos de Red Hat instalados.
- Los certificados `/etc/pki/consumer` identifican la cuenta de Red Hat para el registro.
- Los certificados `/etc/pki/entitlement` indican cuáles son las suscripciones que están adjuntadas.

El comando `rct` inspecciona los certificados y el comando `subscription-manager` examina las suscripciones adjuntas en el sistema.



Referencias

Páginas del manual: `subscription-manager(8)` y `rct(8)`

Para obtener más información, consulte *Registering the System and Managing Subscriptions* en

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/configuring_basic_system_settings/assembly_registering-the-system-and-managing-subscriptions_configuring-basic-system-settings

► Cuestionario

Registro de sistemas para Soporte de Red Hat

Elija la respuesta correcta para las siguientes preguntas:

- ▶ 1. **¿Qué ítem ayuda a registrar el sistema en Red Hat Subscription Management sin un nombre de usuario y una contraseña?**
 - a. ID de la organización
 - b. URL del proxy
 - c. Claves de activación
 - d. dnf

- ▶ 2. **¿Qué herramienta GUI se usa para registrar y suscribir un sistema?**
 - a. PackageKit
 - b. gpk-application
 - c. Red Hat Subscription Manager
 - d. gnome-software

- ▶ 3. **¿Qué directorio almacena los certificados para los productos de Red Hat cuando se usan certificados de derechos (entitlements)?**
 - a. /etc/pki/entitlement
 - b. /etc/subscription/product
 - c. /etc/pki/product
 - d. /etc/certs/pki
 - e. Ninguna de las opciones anteriores.

► Solución

Registro de sistemas para Soporte de Red Hat

Elija la respuesta correcta para las siguientes preguntas:

- ▶ 1. **¿Qué ítem ayuda a registrar el sistema en Red Hat Subscription Management sin un nombre de usuario y una contraseña?**
 - a. ID de la organización
 - b. URL del proxy
 - c. Claves de activación
 - d. dnf
- ▶ 2. **¿Qué herramienta GUI se usa para registrar y suscribir un sistema?**
 - a. PackageKit
 - b. gpk-application
 - c. Red Hat Subscription Manager
 - d. gnome-software
- ▶ 3. **¿Qué directorio almacena los certificados para los productos de Red Hat cuando se usan certificados de derechos (entitlements)?**
 - a. /etc/pki/entitlement
 - b. /etc/subscription/product
 - c. /etc/pki/product
 - d. /etc/certs/pki
 - e. Ninguna de las opciones anteriores.

Instalación y actualización de paquetes de software con DNF

Objetivos

Buscar, instalar y actualizar paquetes de software con el comando dnf.

Administración de paquetes de software con DNF

DNF (Dandified YUM) reemplazó a YUM como administrador de paquetes en Red Hat Enterprise Linux 9. Funcionalmente, los comandos DNF son los mismos que los comandos YUM. Por razones de compatibilidad, los comandos YUM aún existen como enlaces simbólicos a DNF:

```
[user@host ~]$ ls -l /bin/ | grep yum | awk '{print $9 " " $10 " " $11}'
yum -> dnf-3
yum-builddep -> /usr/libexec/dnf-utils
yum-config-manager -> /usr/libexec/dnf-utils
yum-debug-dump -> /usr/libexec/dnf-utils
yum-debug-restore -> /usr/libexec/dnf-utils
yumdownloader -> /usr/libexec/dnf-utils
yum-groups-manager -> /usr/libexec/dnf-utils
```

En este curso, trabajará con el comando dnf. Es posible que parte de la documentación haga referencia al comando yum, pero los archivos son el mismo comando vinculado.

El comando de bajo nivel rpm se puede usar para instalar paquetes, pero no está diseñado para trabajar con repositorios de paquetes o para resolver dependencias de múltiples fuentes automáticamente.

DNF mejora la instalación y las actualizaciones de software basadas en RPM. Con el comando dnf, puede instalar, actualizar, eliminar y obtener información sobre los paquetes de software y sus dependencias. Puede obtener un historial de transacciones realizadas y trabajar con múltiples repositorios de software de Red Hat y terceros.

Buscar software con DNF

El comando dnf help muestra información sobre el uso. El comando dnf list muestra los paquetes instalados y aquellos disponibles.

```
[user@host ~]$ dnf list 'http*'
Available Packages
http-parser.i686          2.9.4-6.el9    rhel-9.0-for-x86_64-appstream-rpms
http-parser.x86_64          2.9.4-6.el9    rhel-9.0-for-x86_64-appstream-rpms
httpcomponents-client.noarch 4.5.13-2.el9  rhel-9.0-for-x86_64-appstream-rpms
httpcomponents-core.noarch   4.4.13-6.el9  rhel-9.0-for-x86_64-appstream-rpms
httpd.x86_64                2.4.51-5.el9  rhel-9.0-for-x86_64-appstream-rpms
httpd-devel.x86_64          2.4.51-5.el9  rhel-9.0-for-x86_64-appstream-rpms
httpd-filesystem.noarch      2.4.51-5.el9  rhel-9.0-for-x86_64-appstream-rpms
httpd-manual.noarch         2.4.51-5.el9  rhel-9.0-for-x86_64-appstream-rpms
httpd-tools.x86_64           2.4.51-5.el9  rhel-9.0-for-x86_64-appstream-rpms
```

capítulo 8 | Instalación y actualización de paquetes de software

El comando `dnf search KEYWORD` enumera paquetes por palabras claves 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, use `search all`:

```
[user@host ~]$ dnf search all 'web server'
=====
Summary & Description Matched: web server =====
nginx.x86_64 : A high performance web server and reverse proxy server
pcp-pmda-weblog.x86_64 : Performance Co-Pilot (PCP) metrics from web server logs
=====
Summary Matched: web server =====
libcurl.x86_64 : A library for getting files from web servers
libcurl.i686 : A library for getting files from web servers
=====
Description Matched: web server =====
freeradius.x86_64 : High-performance and highly configurable free RADIUS server
git-instaweb.noarch : Repository browser in gitweb
http-parser.i686 : HTTP request/response parser for C
http-parser.x86_64 : HTTP request/response parser for C
httpd.x86_64 : Apache HTTP Server
mod_auth_openidc.x86_64 : OpenID Connect auth module for Apache HTTP Server
mod_jk.x86_64 : Tomcat mod_jk connector for Apache
mod_security.x86_64 : Security module for the Apache HTTP Server
varnish.i686 : High-performance HTTP accelerator
varnish.x86_64 : High-performance HTTP accelerator
...output omitted...
```

El comando `dnf info PACKAGE_NAME` arroja información detallada sobre un paquete, que incluye el espacio en disco necesario para la instalación. Por ejemplo, el siguiente comando recupera información acerca del paquete `httpd`:

```
[user@host ~]$ dnf info httpd
Available Packages
Name        : httpd
Version     : 2.4.51
Release     : 5.el9
Architecture: x86_64
Size        : 1.5 M
Source      : httpd-2.4.51-5.el9.src.rpm
Repository  : rhel-9.0-for-x86_64-appstream-rpms
Summary     : Apache HTTP Server
URL         : https://httpd.apache.org/
License     : ASL 2.0
Description  : The Apache HTTP Server is a powerful, efficient, and extensible
               : web server.
```

El comando `dnf provides PATHNAME` muestra paquetes que coinciden con el nombre de ruta especificado (que a menudo, incluye caracteres comodines). Por ejemplo, el siguiente comando busca paquetes que proporcionan el directorio `/var/www/html`:

```
[user@host ~]$ dnf provides /var/www/html
httpd-filesystem-2.4.51-5.el9.noarch : The basic directory layout for the Apache
                                         HTTP Server
Repo       : rhel-9.0-for-x86_64-appstream-rpms
Matched from:
Filename   : /var/www/html
```

Instalar y eliminar software con DNF

El comando `dnf install PACKAGENAME` obtiene e instala un paquete de software junto con cualquier tipo de dependencia.

```
[root@host ~]# dnf install httpd
Dependencies resolved.
=====
 Package      Arch    Version       Repository      Size
=====
Installing:
 httpd        x86_64  2.4.51-5.el9   rhel-9.0-for-x86_64-appstream-rpms 1.5 M
Installing dependencies:
 apr          x86_64  1.7.0-11.el9   rhel-9.0-for-x86_64-appstream-rpms 127 k
 apr-util     x86_64  1.6.1-20.el9   rhel-9.0-for-x86_64-appstream-rpms 98 k
 apr-util-bdb x86_64  1.6.1-20.el9   rhel-9.0-for-x86_64-appstream-rpms 15 k
 httpd-filesystem noarch 2.4.51-5.el9   rhel-9.0-for-x86_64-appstream-rpms 17 k
 httpd-tools   x86_64  2.4.51-5.el9   rhel-9.0-for-x86_64-appstream-rpms 88 k
 redhat-logos-httdp
                  noarch 90.4-1.el9    rhel-9.0-for-x86_64-appstream-rpms 18 k
Installing weak dependencies:
 apr-util-openssl x86_64 1.6.1-20.el9   rhel-9.0-for-x86_64-appstream-rpms 17 k
 mod_http2       x86_64  1.15.19-2.el9   rhel-9.0-for-x86_64-appstream-rpms 153 k
 mod_lua         x86_64  2.4.51-5.el9   rhel-9.0-for-x86_64-appstream-rpms 63 k

Transaction Summary
=====
Install 10 Packages

Total download size: 2.1 M
Installed size: 5.9 M
Is this ok [y/N]: y
Downloading Packages:
(1/10): apr-1.7.0-11.el9.x86_64.rpm           6.4 MB/s | 127 kB   00:00
(2/10): apr-util-bdb-1.6.1-20.el9.x86_64.rpm   625 kB/s |  15 kB   00:00
(3/10): apr-util-openssl-1.6.1-20.el9.x86_64.r p 1.9 MB/s |  17 kB   00:00
...output omitted...
Total                                         24 MB/s | 2.1 MB   00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :                                                 1/1
  Installing    : apr-1.7.0-11.el9.x86_64           1/10
  Installing    : apr-util-bdb-1.6.1-20.el9.x86_64   2/10
  Installing    : apr-util-openssl-1.6.1-20.el9.x86_64 3/10
...output omitted...
Installed:
  apr-1.7.0-11.el9.x86_64           apr-util-1.6.1-20.el9.x86_64
  apr-util-bdb-1.6.1-20.el9.x86_64   apr-util-openssl-1.6.1-20.el9.x86_64
...output omitted...
Complete!
```

capítulo 8 | Instalación y actualización de paquetes de software

El comando `dnf update PACKAGE NAME` obtiene e instala una versión más reciente del paquete especificado, 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 nombre anterior no funcionará después de la actualización. Si no se especifica el PACKAGE NAME, instala todas las actualizaciones relevantes.

```
[root@host ~]# dnf update
```

Dado que un kernel nuevo puede evaluarse solo mediante el inicio en ese kernel, el paquete soporta específicamente la instalación de múltiples versiones simultáneamente. Si el kernel nuevo no arranca, el kernel anterior sigue estando disponible. La ejecución del comando `dnf update kernel` instala el nuevo kernel. Los archivos de configuración contienen una lista de paquetes que siempre deben instalarse aunque el administrador solicite una actualización.

Use el comando `dnf list kernel` para detallar todos los kernel instalados y disponibles. Para ver el kernel en funcionamiento actualmente, use el comando `uname`. El comando `uname` con la opción `-r` muestra solamente la versión y el lanzamiento del kernel, y el comando `uname` con la opción `-a` muestra el lanzamiento e información adicional del kernel.

```
[user@host ~]$ dnf list kernel
Installed Packages
kernel.x86_64                  5.14.0-70.el9          @System
[user@host ~]$ uname -r
5.14.0-70.el9.x86_64
[user@host ~]$ uname -a
Linux workstation.lab.example.com 5.14.0-70.el9.x86_64 #1 SMP PREEMPT Thu Feb 24
19:11:22 EST 2022 x86_64 x86_64 x86_64 GNU/Linux
```

El comando `dnf remove PACKAGE NAME` elimina un paquete de software instalado, incluido cualquier paquete soportado.

```
[root@host ~]# dnf remove httpd
```



Advertencia

El comando `dnf remove` quita los paquetes enumerados y *cualquier paquete que requiere que se eliminan los paquetes* (y los paquetes que requieren esos paquetes, etc.). Este comando puede dar lugar a una eliminación inesperada de paquetes, por lo que debe verificar detenidamente la lista de paquetes que se quitarán.

Instalar y eliminar grupos de software con DNF

El comando `dnf` 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 9, el comando `dnf` puede instalar dos tipos de grupos de paquetes. Los grupos regulares son colecciones de paquetes. Los grupos de entorno son colecciones de grupos regulares. Los paquetes o grupos proporcionados por estas colecciones pueden ser **mandatory** (deben instalarse si el grupo se instala), **default** (normalmente se instalan si el grupo se instala) o **optional** (no se instalan cuando se instala el grupo a menos que se lo solicite específicamente).

Al igual que el comando `dnf list`, el comando `dnf group list` muestra los nombres de grupos instalados y disponibles.

```
[user@host ~]$ dnf group list
Available Environment Groups:
  Server with GUI
  Server
  Minimal Install
...output omitted...
Available Groups:
  Legacy UNIX Compatibility
  Console Internet Tools
  Container Management
...output omitted...
```

Algunos grupos se instalan normalmente a través de grupos de entorno y se ocultan de manera predeterminada. Muestre los grupos ocultos con el comando `dnf group list hidden`.

El comando `dnf group info` muestra información relacionada con un grupo. Incluye una lista de nombres de paquetes obligatorios, predeterminados u opcionales.

```
[user@host ~]$ dnf group info "RPM Development Tools"
Group: RPM Development Tools
Description: Tools used for building RPMs, such as rpmbuild.
Mandatory Packages:
  redhat-rpm-config
  rpm-build
Default Packages:
  rpmdevtools
Optional Packages:
  rpmlint
```

El comando `dnf group install` instala un grupo que instala sus paquetes obligatorios y predeterminados, y los paquetes de los que depende.

```
[root@host ~]# dnf group install "RPM Development Tools"
...output omitted...
Installing Groups:
  RPM Development Tools

Transaction Summary
=====
Install 19 Packages

Total download size: 4.7 M
Installed size: 15 M
Is this ok [y/N]: y
...output omitted...
```

**Importante**

A partir de Red Hat Enterprise Linux 7, el comportamiento de los grupos Yum cambió para ser tratados como objetos y monitoreados por el sistema. Si un grupo instalado se actualiza y el repositorio Yum agregó paquetes nuevos obligatorios o predeterminados al grupo, dichos paquetes nuevos se instalan 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, o si ningún paquete predeterminado u opcional en el grupo se instaló. A partir de RHEL 7, un grupo se considera instalado solo si se usó `yum group install` para su instalación. Puede usar el comando `yum group mark install GROUPNAME` para marcar un grupo como instalado, y los paquetes faltantes y sus dependencias se instalan 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 `yum group list` equivalente en RHEL 7 y RHEL 8, no.

Visualización del historial de transacciones

Todas las transacciones de instalación y eliminación se registran en el archivo `/var/log/dnf.rpm.log`.

```
[user@host ~]$ tail -5 /var/log/dnf.rpm.log
2022-03-23T16:46:43-0400 SUBDEBUG Installed: python-srpm-macros-3.9-52.el9.noarch
2022-03-23T16:46:43-0400 SUBDEBUG Installed: redhat-rpm-config-194-1.el9.noarch
2022-03-23T16:46:44-0400 SUBDEBUG Installed: elfutils-0.186-1.el9.x86_64
2022-03-23T16:46:44-0400 SUBDEBUG Installed: rpm-build-4.16.1.3-11.el9.x86_64
2022-03-23T16:46:44-0400 SUBDEBUG Installed: rpmdevtools-9.5-1.el9.noarch
```

El comando `dnf history` muestra un resumen de transacciones de instalación y eliminación.

ID	Command line	Date and time	Action(s)	Altered
7	group install RPM Develop	2022-03-23 16:46	Install	20
6	install httpd	2022-03-23 16:21	Install	10 EE
5	history undo 4	2022-03-23 15:04	Removed	20
4	group install RPM Develop	2022-03-23 15:03	Install	20
3		2022-03-04 03:36	Install	5
2		2022-03-04 03:33	Install	767 EE
1	-y install patch ansible-	2022-03-04 03:31	Install	80

El comando `dnf history undo` invierte una transacción.

```
[root@host ~]# dnf history undo 6
...output omitted...
Removing:
  apr-util-openssl x86_64 1.6.1-20.el9 @rhel-9.0-for-x86_64-appstream-rpms 24 k
  httpd           x86_64 2.4.51-5.el9 @rhel-9.0-for-x86_64-appstream-rpms 4.7 M
...output omitted...
```

Resumen de los comandos DNF

Los paquetes pueden ubicarse, instalarse, actualizarse y eliminarse por nombre o por grupos de paquetes.

Tarea:	Comando:
Enumerar paquetes instalados y disponibles por nombre	<code>dnf list [NAME-PATTERN]</code>
Enumerar grupos instalados y disponibles	<code>dnf group list</code>
Buscar un paquete por palabra clave	<code>dnf search KEYWORD</code>
Mostrar detalles de un paquete	<code>dnf info PACKAGE NAME</code>
Instalar un paquete	<code>dnf install PACKAGE NAME</code>
Instalar un grupo de paquetes	<code>dnf group install GROUP NAME</code>
Actualizar todos los paquetes	<code>dnf update</code>
Eliminar un paquete	<code>dnf remove PACKAGE NAME</code>
Mostrar historial de transacciones	<code>dnf history</code>

Administración de flujos de módulos de paquete con DNF

Tradicionalmente, administrar versiones alternativas del paquete de software de una aplicación y sus paquetes relacionados significaba mantener diferentes repositorios para cada versión. Para los desarrolladores que querían la última versión de una aplicación y los administradores que querían la versión más estable de la aplicación, se obtuvo como resultado una situación tediosa de administrar. Red Hat simplifica este proceso mediante el uso de una tecnología denominada *modularidad*. Con la modularidad, un solo repositorio puede alojar varias versiones del paquete de una aplicación y sus dependencias.

Introducción a BaseOS y Application Stream

El contenido de Red Hat Enterprise Linux 9 se distribuye a través de dos repositorios de software principales: *BaseOS* y *Application Stream* (AppStream).

El repositorio de *BaseOS* proporciona el contenido del sistema operativo central (*core*) para Red Hat Enterprise Linux como paquetes RPM. Los componentes de *BaseOS* tienen un ciclo de vida idéntico al del contenido de versiones anteriores de Red Hat Enterprise Linux. El repositorio de *Application Stream* proporciona contenido con distintos ciclos de vida como módulos y paquetes tradicionales.

Application Stream contiene las partes necesarias del sistema, así como una amplia gama de aplicaciones previamente disponibles como parte de Red Hat Software Collections y otros productos y programas. Cada *Application Stream* tiene un ciclo de vida que es el mismo que Red Hat Enterprise Linux 9 o más corto.

Tanto *BaseOS* como *AppStream* son una parte necesaria de un sistema Red Hat Enterprise Linux 9.

El repositorio de Application Stream, contiene dos tipos de contenido: módulos y paquetes RPM tradicionales. Un módulo describe un conjunto de paquetes RPM que están relacionados. Los módulos pueden contener varios flujos para que haya varias versiones de aplicaciones disponibles para la instalación. Al habilitar un flujo de módulos, el sistema tiene acceso a los paquetes RPM dentro de ese flujo de módulos. Normalmente, los módulos se organizan en torno a una versión específica de una aplicación de software o lenguaje de programación. Un módulo típico contiene paquetes con una aplicación, paquetes con las librerías de dependencia específica de la aplicación, paquetes con documentación para la aplicación y paquetes con utilidades auxiliares.



Importante

Red Hat Enterprise Linux 9.0 se envía sin módulos. Las versiones futuras de RHEL 9 pueden incluir contenido adicional y versiones de software posteriores como módulos. Además, a partir de RHEL 9, debe especificar manualmente los flujos de módulos predeterminados, ya que ya no están definidos de forma predeterminada. Puede definir flujos de módulos predeterminados con archivos de configuración en el directorio `/etc/dnf/modules.defaults.d/`.

Flujos de módulos

Cada módulo tiene uno o más *flujos de módulos*, que contienen diferentes versiones del contenido. Cada uno de los flujos recibe actualizaciones de forma independiente. Piense en el flujo de módulos como un repositorio virtual en el repositorio físico del flujo de aplicaciones.

Para cada módulo, solo puede habilitarse uno de sus flujos, y este flujo proporciona sus paquetes.

Perfiles de módulos

Cada módulo puede tener uno o más perfiles. Un perfil es una lista de paquetes que se deben instalar juntos para un determinado caso de uso por ejemplo, para un servidor, cliente, desarrollo, instalación mínima u otro.

La instalación de un perfil de módulo particular simplemente instala un conjunto particular de paquetes desde el flujo del módulo. Posteriormente puede instalar o desinstalar paquetes normalmente. Si no especifica un perfil, el módulo instalará su perfil predeterminado.

Administración de flujos con DNF

Red Hat Enterprise Linux 9 agrega características modulares de Application Stream. Para manejar el contenido modular, puede usar el comando `dnf module`. De lo contrario, el comando `dnf` funciona con módulos similares a los paquetes regulares.

Puede encontrar algunos comandos importantes al administrar módulos en la siguiente lista:

- **`dnf module list`**: enumera los módulos disponibles con el nombre del módulo, el flujo, los perfiles y un resumen.
- **`dnf module list module-name`**: enumera los flujos de módulos para un módulo específico y recupera su estado.
- **`dnf module info module-name`**: muestra los detalles de un módulo, incluidos los perfiles disponibles y una lista de los paquetes que instala el módulo. La ejecución del comando `dnf module info` sin especificar un flujo de módulo enumera los paquetes que se instalan desde el perfil y el flujo predeterminados. Use el formato `module-name:stream` para ver un flujo de módulos específico. Agregue la opción `--profile` para mostrar información sobre los paquetes instalados por cada uno de los perfiles del módulo.

- **dnf module provides package** : muestra qué módulo proporciona un paquete específico.



Referencias

Páginas del manual: `dnf(1)` y `dnf.conf(5)`

Para obtener más información, consulte el capítulo *Managing Software Packages* de la *Red Hat Enterprise Linux 9 Configuring Basic system Settings Guide* en https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/configuring_basic_system_settings/index#managing-software-packages_configuring-basic-system-settings

Para obtener más información, consulte el capítulo *Distribution of Content in RHEL 9* de la *Red Hat Enterprise Linux 9 Managing Software with the DNF Tool Guide* en https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/managing_software_with_the_dnf_tool/index#assembly_distribution-of-content-in-rhel-9_managing-software-with-the-dnf-tool

Modularidad

<https://docs.fedoraproject.org/en-US/modularity/>

► Ejercicio Guiado

Instalación y actualización de paquetes de software con DNF

En este ejercicio, instala y quita paquetes y grupos de paquetes.

Resultados

- Instalar y eliminar paquetes con dependencias.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start software-dnf
```

Instrucciones

- 1. Desde `workstation`, abra una sesión de SSH en la máquina `servera` como el usuario `student`. Use el comando `sudo -i` para cambiar al usuario `root`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ sudo -i
Password: student
[root@servera ~]#
```

- 2. Busque un paquete específico.

- 2.1. Intente ejecutar el comando `nmap`. Se le indicará que no está instalado.

```
[root@servera ~]# nmap
-bash: nmap: command not found
```

- 2.2. Use el comando `dnf search` para buscar paquetes con `nmap` como parte de su nombre o resumen.

```
[root@servera ~]# dnf search nmap
...output omitted...
===== Name Exactly Matched: nmap =====
nmap.x86_64 : Network exploration tool and security scanner
===== Name & Summary Matched: nmap =====
nmap-ncat.x86_64 : Nmap's Netcat replacement
```

- 2.3. Use el comando `dnf info` para obtener más información acerca del paquete `nmap`.

```
[root@servera ~]# dnf info nmap
...output omitted...
Available Packages
Name        : nmap
Epoch       : 3
Version    : 7.91
Release    : 10.el9
...output omitted...
```

► 3. Use el comando `dnf install` para instalar el paquete `nmap`.

```
[root@servera ~]# dnf install nmap
...output omitted...
Dependencies resolved.
=====
Package          Arch      Version       Repository      Size
=====
Installing:
  nmap     x86_64    3:7.91-10.el9    rhel-9.0-for-x86_64-appstream-rpms  5.6 M

Transaction Summary
=====
Install 1 Package

Total download size: 5.6 M
Installed size: 24 M
Is this ok [y/N]: y
...output omitted...
Complete!
```

► 4. Quite paquetes.

- 4.1. Use el comando `dnf remove` para eliminar el paquete `nmap`, pero responda con `no` cuando se le solicite. ¿Cuántos paquetes se quitan?

```
[root@servera ~]# dnf remove nmap
Dependencies resolved.
=====
Package          Arch      Version       Repository      Size
=====
Removing:
  nmap     x86_64    3:7.91-10.el9    @rhel-9.0-for-x86_64-appstream-rpms  24 M

Transaction Summary
=====
Remove 1 Package
```

```
Freed space: 24 M
Is this ok [y/N]: n
Operation aborted.
```

- 4.2. Use el comando `dnf remove` para eliminar el paquete `tar`, pero responda con no cuando se le solicite. ¿Cuántos paquetes se quitan?

```
[root@servera ~]# dnf remove tar
...output omitted...
Dependencies resolved.
=====
 Package      Arch    Version       Repository      Size
 -----
Removing:
 tar          x86_64  2:1.34-3.el9   @System           3.0 M
Removing dependent packages:
 cockpit      x86_64  264-1.el9     @rhel-9.1-for-x86_64-baseos-rpms  57 k
 cockpit-system noarch 264-1.el9     @System           3.3 M
...output omitted...

Transaction Summary
=====
Remove 12 Packages

Freed space: 48 M
Is this ok [y/N]: n
Operation aborted.
```

- 5. Recopile información sobre el grupo de componentes de "Herramientas de seguridad" e instálelo en `servera`.

- 5.1. Use el comando `dnf group list` para enumerar todos los grupos de componentes disponibles.

```
[root@servera ~]# dnf group list
```

- 5.2. Use el comando `dnf group info` para obtener más información acerca del grupo de componentes `Security Tools`, incluida una lista de paquetes incluidos.

```
[root@servera ~]# dnf group info "Security Tools"
...output omitted...
Group: Security Tools
Description: Security tools for integrity and trust verification.
Default Packages:
  scap-security-guide
Optional Packages:
  aide
  hmaccalc
  openscap
  openscap-engine-sce
  openscap-utils
  scap-security-guide-doc
  scap-workbench
```

capítulo 8 | Instalación y actualización de paquetes de software

```
tpm2-tools
tss2
udica
```

- 5.3. Use el comando `dnf group install` para instalar el grupo de componentes Security Tools.

```
[root@servera ~]# dnf group install "Security Tools"
...output omitted...
Dependencies resolved.
=====
Package           Arch    Version      Repository      Size
=====
Installing group/module packages:
scap-security-guide
noarch 0.1.60-5.el9   rhel-9.0-for-x86_64-appstream-rpms 683 k
Installing dependencies:
openscap          x86_64  1:1.3.6-3.el9  rhel-9.0-for-x86_64-appstream-rpms 2.0 M
...output omitted...

Transaction Summary
=====
Install  5 Packages

Total download size: 3.0 M
Installed size: 94 M
Is this ok [y/N]: y
...output omitted...
Installed:
  openscap-1:1.3.6-3.el9.x86_64
  openscap-scanner-1:1.3.6-3.el9.x86_64
  scap-security-guide-0.1.60-5.el9.noarch
  xmlsec1-1.2.29-9.el9.x86_64
  xmlsec1-openssl-1.2.29-9.el9.x86_64

Complete!
```

- 6. Explore el historial y las opciones de anulación del comando `dnf`.

- 6.1. Use el comando `dnf history` para mostrar el historial de `dnf` reciente.

```
[root@servera ~]# dnf history
ID      | Command line           | Date and time     | Action(s)      | Altered
-----
3 | group install Security T | 2022-03-24 15:23 | Install        | 6
2 | install nmap            | 2022-03-24 15:12 | Install        | 1
1 | -y install @base firewall | 2022-03-03 04:47 | Install        | 156 EE
```

En su sistema, es probable que el historial sea diferente.

- 6.2. Use el comando `dnf history info` para confirmar que la última transacción sea la instalación del grupo. En el siguiente comando, reemplace el ID de transacción por el que se menciona en el paso anterior.

```
[root@servera ~]# dnf history info 3
Transaction ID : 3
Begin time     : Thu 24 Mar 2022 03:23:56 PM EDT
Begin rpmdb    : 7743aed72ac79f632442c9028aafdf2499a1591f92a660b3f09219b422ca95f02
End time       : Thu 24 Mar 2022 03:23:58 PM EDT (2 seconds)
End rpmdb      : 20c4f021538b7dca9a874260784b1e5cf9bc142da869967269e3d84dd0f789d
User          : Student User <student>
Return-Code    : Success
Releasever    : 9
Command Line   : group install Security Tools
Comment        :
Packages Altered:
  Install openscap-1:1.3.6-3.el9.x86_64           @rhel-9.0-for-x86_64-
appstream-rpms
  Install openscap-scanner-1:1.3.6-3.el9.x86_64   @rhel-9.0-for-x86_64-
appstream-rpms
...output omitted...
```

- 6.3. Use el comando `dnf history undo` para eliminar el conjunto de paquetes que se instalaron cuando se instaló el paquete `nmap`. En su sistema, busque el ID de transacción correcto de la salida del comando `dnf history` y luego, use ese ID en el siguiente comando.

```
[root@servera ~]# dnf history undo 2
```

- 7. Regrese al sistema `workstation` como el usuario `student`.

```
[root@servera ~]# exit
logout
[student@servera ~]$ exit
Connection to servera closed.
[student@workstation ~]$
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish software-dnf
```

Esto concluye la sección.

Habilitar repositorios de software con DNF

Objetivos

Habilitar y deshabilitar el uso de repositorios DNF de terceros o de Red Hat por un servidor.

Habilitación de repositorios de software de Red Hat

En muchos casos, los sistemas tienen acceso a numerosos repositorios de Red Hat. El comando `dnf repolist all` enumera todos los repositorios disponibles y sus estados:

```
[user@host ~]$ dnf repolist all
repo id                                repo name          status
rhel-9.0-for-x86_64-appstream-rpms      RHEL 9.0 AppStream    enabled
rhel-9.0-for-x86_64-baseos-rpms        RHEL 9.0 BaseOS      enabled
```



nota

Las suscripciones a Red Hat otorgan acceso a repositorios específicos. En el pasado, los administradores necesitaban adjuntar suscripciones por sistema. Acceso a Contenido Simple (SCA) simplifica la forma en que los sistemas acceden a los repositorios. Con SCA, los sistemas pueden acceder a cualquier repositorio desde cualquier suscripción que adquiera, sin necesidad de asociar una suscripción. Puede habilitar SCA en el portal de clientes de Red Hat dentro de [My Subscriptions > Subscription Allocations](#) o en su servidor de Red Hat Satellite.

El comando `dnf config-manager` puede habilitar o deshabilitar los repositorios. Por ejemplo, el siguiente comando habilita el repositorio `rhel-9-server-debug-rpms`:

```
[user@host ~]$ dnf config-manager --enable rhel-9-server-debug-rpms
```

Las fuentes que no son de Red Hat proporcionan software a través de repositorios de terceros. Por ejemplo, Adobe proporciona parte de su software para Linux a través de repositorios DNF. En un aula Red Hat, el servidor `content.example.com` aloja repositorios DNF. El comando `dnf` puede acceder a los repositorios desde un sitio web, un servidor FTP o el sistema de archivos local.

Puede agregar un repositorio de terceros de dos maneras. Puede crear un archivo `.repo` en el directorio `/etc/yum.repos.d/` o puede agregar una sección `[repository]` al archivo `/etc/dnf/dnf.conf`. Red Hat recomienda usar archivos `.repo` y reservar el archivo `dnf.conf` para configuraciones de repositorio adicionales. El comando `dnf` busca ambas ubicaciones de manera predeterminada; sin embargo, los archivos `.repo` tienen prioridad. Un archivo `.repo` 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.

Agregar repositorios DNF

El comando `dnf config-manager` también puede agregar repositorios a la máquina. El siguiente comando crea un archivo `.repo` mediante el uso de la URL de un repositorio existente.

```
[user@host ~]$ dnf config-manager \
--add-repo="https://dl.fedoraproject.org/pub/epel/9/Everything/x86_64/"
Adding repo from: https://dl.fedoraproject.org/pub/epel/9/Everything/x86_64/
```

El archivo .repo correspondiente está visible en el directorio /etc/yum.repos.d/:

```
[user@host ~]$ cd /etc/yum.repos.d
[user@host yum.repos.d]$ cat \
dl.fedoraproject.org_pub_epel_9_Everything_x86_64_.repo
[dl.fedoraproject.org_pub_epel_9_Everything_x86_64_]
name=created by dnf config-manager from https://dl.fedoraproject.org/pub/epel/9/
Everything/x86_64/
baseurl=https://dl.fedoraproject.org/pub/epel/9/Everything/x86_64/
enabled=1
```

Modifique este archivo para personalizar los parámetros y especificar la ubicación de una clave GPG. Las claves se almacenan en diversas ubicaciones en el sitio del repositorio remoto, como http://dl.fedoraproject.org/pub/epel/RPM-GPG-KEY-EPEL-9. Los administradores deberían descargar la clave en un archivo local en lugar de permitir que el comando `dnf` la recupere de una fuente externa. Por ejemplo, el siguiente archivo .repo usa el parámetro `gpgkey` para hacer referencia a una clave local:

```
[EPEL]
name=EPEL 9
baseurl=https://dl.fedoraproject.org/pub/epel/9/Everything/x86_64/
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-9
```

Paquetes de configuración de RPM para repositorios locales

Algunos repositorios proporcionan este archivo de configuración y la clave pública de GPG como parte del paquete de RPM para simplificar su instalación. El comando `dnf install` puede descargar e instalar estos paquetes RPM.

Por ejemplo, el siguiente comando instala el RPM del repositorio RHEL9 Extra Packages for Enterprise Linux (EPEL):

```
[user@host ~]$ rpm --import \
http://dl.fedoraproject.org/pub/epel/RPM-GPG-KEY-EPEL-9
[user@host ~]$ dnf install \
https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

Los archivos .repo suelen enumerar varias referencias de repositorio en un solo archivo. Cada referencia de repositorio comienza con un nombre de una sola palabra entre corchetes.

```
[user@host ~]$ cat /etc/yum.repos.d/epel.repo
[epel]
name=Extra Packages for Enterprise Linux $releasever - $basearch
#baseurl=https://download.example/pub/epel/$releasever/Everything/$basearch/
metalink=https://mirrors.fedoraproject.org/metalink?repo=epel-$releasever&arch=
$basearch&infra=$infra&content=$contentdir
```

```

enabled=1
gpgcheck=1
countme=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-$releasever
...output omitted...
[epel-source]
name=Extra Packages for Enterprise Linux $releasever - $basearch - Source
#baseurl=https://download.example/pub/epel/$releasever/Everything/source/tree/
metalink=https://mirrors.fedoraproject.org/metalink?repo=epel-source-
$releasever&arch=$basearch&infra=$infra&content=$contentdir
enabled=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-$releasever
gpgcheck=1

```

Para definir un repositorio, pero no buscarlo de forma predeterminada, inserte el parámetro `enabled=0`. Si bien el comando `dnf config-manager` habilita y deshabilita los repositorios de manera persistente, el comando `dnf` con las opciones `--enablerrepo= PATTERN` y `--disablerepo= PATTERN` es temporal mientras dura el comando.



Advertencia

Instale la clave GPG de RPM antes de instalar los paquetes firmados, para asegurarse de que los paquetes provengan de una fuente confiable. Si la clave GPG de RPM no está instalada, el comando `dnf` no puede instalar los paquetes firmados. El comando `dnf` con la opción `--nogpgcheck` ignora las claves GPG que faltan, pero puede resultar en la instalación de paquetes comprometidos o falsificados.



Referencias

Páginas del manual: `dnf(8)`, `dnf.conf(5)` y `dnf-config-manager(8)`

Para obtener más información, consulte el capítulo *Managing Software with the DNF Tool* en la documentación del producto Red Hat Enterprise Linux 9 en https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/managing_software_with_the_dnf_tool

► Ejercicio Guiado

Habilitar repositorios de software con DNF

En este ejercicio, configurará su servidor para obtener paquetes desde un repositorio DNF remoto, luego actualizará o instalará un paquete desde ese repositorio.

Resultados

- Configurar un sistema para obtener actualizaciones de software de un servidor de aula y actualizar el sistema para usar los paquetes más recientes.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start software-repo
```

Instrucciones

- 1. Use el comando `ssh` para iniciar sesión en el sistema `servera` con el usuario `student`. Use el comando `sudo -i` para cambiar al usuario `root`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

- 2. Configure repositorios de software en `servera` para obtener paquetes personalizados y actualizaciones desde la siguiente URL:

- Paquetes personalizados proporcionados en `http://content.example.com/rhel9.0/x86_64/rhcsa-practice/rht`
 - Actualizaciones de paquetes personalizados proporcionados en `http://content.example.com/rhel9.0/x86_64/rhcsa-practice/errata`
- 2.1. Use el comando `dnf config-manager` para agregar el repositorio de paquetes personalizado.

```
[root@servera ~]# dnf config-manager \
--add-repo "http://content.example.com/rhel9.0/x86_64/rhcsa-practice/rht"
Adding repo from: http://content.example.com/rhel9.0/x86_64/rhcsa-practice/rht
```

- 2.2. Examine el archivo de repositorio de software que el comando anterior creó en el directorio /etc/yum.repos.d. Use el comando vim para editar el archivo y agregue el parámetro gpgcheck=0 para deshabilitar la comprobación de clave GPG para el repositorio.

```
[root@servera ~]# vim \
/etc/yum.repos.d/content.example.com_rhel9.0_x86_64_rhcsa-practice_rht.repo
[content.example.com_rhel9.0_x86_64_rhcsa-practice_rht]
name=created by dnf config-manager from http://content.example.com/rhel9.0/x86_64/
rhcsa-practice/rht
baseurl=http://content.example.com/rhel9.0/x86_64/rhcsa-practice/rht
enabled=1
gpgcheck=0
```

- 2.3. Cree el archivo /etc/yum.repos.d/errata.repo para habilitar el repositorio de actualizaciones con el siguiente contenido:

```
[rht-updates]
name=rht updates
baseurl=http://content.example.com/rhel9.0/x86_64/rhcsa-practice/errata
enabled=1
gpgcheck=0
```

- 2.4. Use el comando dnf repolist all para enumerar todos los repositorios en el sistema.

```
[root@servera ~]# dnf repolist all
repo id                                repo name      status
content.example.com_rhel9.0_x86_64_rhcsa-practice_rht  created by .... enabled
...output omitted...
rht-updates                               rht updates    enabled
```

► 3. Deshabilite el repositorio de software rht-updates e instale el paquete rht-system.

- 3.1. Use el comando dnf config-manager --disable para deshabilitar el repositorio rht-updates.

```
[root@servera ~]# dnf config-manager --disable rht-updates
```

- 3.2. Muestre el paquete rht-system y, luego, instálelo.

```
[root@servera ~]# dnf list rht-system
Available Packages
rht-system.noarch  1.0.0-1 content.example.com_rhel9.0_x86_64_rhcsa-practice_rht
[root@servera ~]# dnf install rht-system
Dependencies resolved.
=====
Package          Arch      Version       Repository      Size
=====
Installing:
  rht-system      noarch   1.0.0-1      content..._rht  3.7 k
...output omitted...
```

```
Is this ok [y/N]: y
...output omitted...
Installed:
  rht-system-1.0.0-1.noarch
Complete!
```

- 3.3. Verifique que el paquete `rht-system` esté instalado y anote el número de versión del paquete.

```
[root@servera ~]# dnf list rht-system
Installed Packages
rht-system.noarch 1.0.0-1 @content.example.com_rhel9.0_x86_64_rhcsa-practice_rht
```

- 4. Habilite el repositorio de software `rht-updates` y actualice todos los paquetes de software relevantes.
- 4.1. Use `dnf config-manager --enable` para habilitar el repositorio `rht-updates`.

```
[root@servera ~]# dnf config-manager --enable rht-updates
```

- 4.2. Use el comando `dnf update` para actualizar todos los paquetes de software en servera.

```
[root@servera ~]# dnf update
Dependencies resolved.
=====
Package           Arch      Version       Repository      Size
=====
Upgrading:
  rht-system      noarch   1.0.0-2      rht-updates    7.5 k
...output omitted...
Is this ok [y/N]: y
...output omitted...
Complete!
```

- 4.3. Verifique que el paquete `rht-system` esté actualizado y anote el número de versión del paquete.

```
[root@servera ~]# dnf list rht-system
Installed Packages
rht-system.noarch          1.0.0-2          @rht-updates
```

- 5. Salga de servera.

```
[root@servera ~]# exit
logout
[student@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish software-repo
```

Esto concluye la sección.

► Trabajo de laboratorio

Instalación y actualización de paquetes de software

En este trabajo de laboratorio, administrará repositorios de software, e instalará y actualizará paquetes de esos repositorios.

Resultados

- Administrar repositorios de software.
- Instalar y actualizar paquetes desde repositorios.
- Instalar un paquete RPM.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start software-review
```

Instrucciones

1. En la máquina `serverb`, configure un repositorio de software para obtener actualizaciones. Otorgue el nombre `errata` al repositorio y configure el repositorio en el archivo `/etc/yum.repos.d/errata.repo`. Configure el archivo `errata.repo` para usar el repositorio `http://content.example.com/rhel9.0/x86_64/rhcsa-practice/errata`. No controle las firmas de GPG.
2. En `serverb`, instale el paquete `rht-system`.
3. Por razones de seguridad, la máquina `serverb` no deberá ser capaz de conectarse a una impresora de papel. Puede lograrlo al eliminar el paquete `cups`. Cuando finalice, salga de la shell `root`.
4. El script de inicio descarga el paquete `rhcsa-script-1.0.0-1.noarch.rpm` en el directorio `/home/student` en la máquina `serverb`. Confirme que el paquete `rhcsa-script-1.0.0-1.noarch.rpm` esté disponible en `serverb` e instálelo con privilegios de `root`. Verifique que el paquete esté instalado. Salga de la máquina `serverb`.

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade software-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish software-review
```

Esto concluye la sección.

► Solución

Instalación y actualización de paquetes de software

En este trabajo de laboratorio, administrará repositorios de software, e instalará y actualizará paquetes de esos repositorios.

Resultados

- Administrar repositorios de software.
- Instalar y actualizar paquetes desde repositorios.
- Instalar un paquete RPM.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start software-review
```

Instrucciones

1. En la máquina `serverb`, configure un repositorio de software para obtener actualizaciones. Otorgue el nombre `errata` al repositorio y configure el repositorio en el archivo `/etc/yum.repos.d/errata.repo`. Configure el archivo `errata.repo` para usar el repositorio `http://content.example.com/rhel9.0/x86_64/rhcsa-practice/errata`. No controle las firmas de GPG.
 - 1.1. Inicie sesión en la máquina `serverb` como el usuario `student` y cambie al usuario `root`.

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
[student@serverb ~]$ sudo -i
[sudo] password for student: student
[root@serverb ~]#
```

- 1.2. Cree el archivo `/etc/yum.repos.d/errata.repo` con el siguiente contenido:

```
[errata]
name=Red Hat Updates
baseurl=http://content.example.com/rhel9.0/x86_64/rhcsa-practice/errata
enabled=1
gpgcheck=0
```

2. En **serverb**, instale el paquete **rht-system**.

2.1. Enumere los paquetes disponibles para el paquete **rht-system**.

```
[root@serverb ~]# dnf list rht-system
Last metadata expiration check: 0:05:27 ago on Wed 27 Apr 2022 05:01:59 AM EDT.
Available Packages
rht-system.noarch      1.0.0-2                  errata
```

2.2. Instale la última versión del paquete **rht-system**.

```
[root@serverb ~]# dnf install rht-system
...output omitted...
Total download size: 7.5 k
Installed size: 300
Is this ok [y/N]: y
...output omitted...
Complete!
[root@serverb ~]#
```

3. Por razones de seguridad, la máquina **serverb** no deberá ser capaz de conectarse a una impresora de papel. Puede lograrlo al eliminar el paquete **cups**. Cuando finalice, salga de la shell **root**.

3.1. Indique el paquete **cups** instalado.

```
[root@serverb ~]# dnf list cups
Last metadata expiration check: 0:08:02 ago on Wed 27 Apr 2022 05:01:59 AM EDT.
Installed Packages
cups.x86_64          1:2.3.3op2-13.el9      @rhel-9.0-for-x86_64-appstream-rpms
[root@serverb ~]#
```

3.2. Elimine el paquete **cups**.

```
[root@serverb ~]# dnf remove cups.x86_64
...output omitted...
Remove 46 Packages

Freed space: 94 M
Is this ok [y/N]: y
...output omitted...
Complete!
```

3.3. Salga de la shell **root**.

```
[root@serverb ~]# exit
[student@serverb ~]$
```

4. El script de inicio descarga el paquete **rhcsa-script-1.0.0-1.noarch.rpm** en el directorio **/home/student** en la máquina **serverb**.

Confirme que el paquete `rhcsa-script-1.0.0-1.noarch.rpm` esté disponible en `serverb` e instálelo con privilegios de `root`. Verifique que el paquete esté instalado. Salga de la máquina `serverb`.

- 4.1. Verifique que el paquete `rhcsa-script-1.0.0-1.noarch.rpm` no esté disponible en `serverb`.

```
[student@serverb ~]$ rpm -q -p rhcsa-script-1.0.0-1.noarch.rpm -i
Name        : rhcsa-script
Version     : 1.0.0
Release     : 1
Architecture: noarch
Install Date: (not installed)
Group       : System
Size        : 593
License     : GPL
Signature   : (none)
Source RPM  : rhcsa-script-1.0.0-1.src.rpm
Build Date  : Wed 23 Mar 2022 08:24:21 AM EDT
Build Host  : localhost
Packager    : Bernardo Gargallo
URL         : http://example.com
Summary     : RHCSA Practice Script
Description  :
A RHCSA practice script.
The package changes the motd.
```

- 4.2. Instale el paquete `rhcsa-script-1.0.0-1.noarch.rpm`.

```
[student@serverb ~]$ sudo dnf install \
rhcsa-script-1.0.0-1.noarch.rpm
[sudo] password for student: student
Last metadata expiration check: 0:11:06 ago on Wed 27 Apr 2022 05:01:59 AM EDT.
Dependencies resolved.
=====
Package      Architecture Version      Repository      Size
=====
Installing:
  rhcsa-script    noarch      1.0.0-1          @commandline  7.5 k

Transaction Summary
=====
Install 1 Package

Total size: 7.5 k
Installed size: 593
Is this ok [y/N]: y
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing       : 1/1
```

```
Running scriptlet: rhcsa-script-1.0.0-1.noarch           1/1
Installing       : rhcsa-script-1.0.0-1.noarch           1/1
Running scriptlet: rhcsa-script-1.0.0-1.noarch           1/1
Verifying       : rhcsa-script-1.0.0-1.noarch           1/1

Installed:
  rhcsa-script-1.0.0-1.noarch

Complete!
```

4.3. Verifique que el paquete esté instalado.

```
[student@serverb ~]$ rpm -q rhcsa-script
rhcsa-script-1.0.0-1.noarch
[student@serverb ~]$
```

4.4. Regrese al sistema `workstation` como el usuario `student`.

```
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@workstation ~]$
```

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade software-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish software-review
```

Esto concluye la sección.

Resumen

- Red Hat Subscription Management proporciona herramientas para que los equipos tengan derecho a suscripciones de productos, obtengan actualizaciones de paquetes de software y busquen información sobre contratos de soporte y suscripciones usadas por sus sistemas.
- La utilidad `dnf` es una herramienta eficaz de la línea de comandos que puede usarse para instalar, actualizar, eliminar y consultar los paquetes de software.
- Puede usar el comando `dnf config-manager` para habilitar y deshabilitar repositorios DNF.

capítulo 9

Administración de almacenamiento básico

Meta

Crear y administrar dispositivos de almacenamiento, particiones, sistemas de archivos y espacios de intercambio (swap) desde la línea de comandos.

Objetivos

- Acceder al contenido de sistemas de archivos mediante la adición y la eliminación de sistemas de archivos de la jerarquía de sistemas de archivos.
- Crear particiones de almacenamiento, formatearlas con sistemas de archivos y montarlas para su uso.
- Crear y administrar espacios de intercambio (swap) para complementar la memoria física.

Secciones

- Montaje y desmontaje de sistemas de archivos (y ejercicio guiado)
- Adición de particiones, sistemas de archivos y montajes persistentes (y ejercicio guiado)
- Administración de espacio de intercambio (swap) (y ejercicio guiado)

Trabajo de laboratorio

- Administración de almacenamiento básico

Montaje y desmontaje de sistemas de archivos

Objetivos

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

Para acceder al sistema de archivos en un dispositivo de almacenamiento extraíble, debe montar el dispositivo de almacenamiento. Con el comando `mount`, el usuario `root` puede montar un sistema de archivos manualmente. El primer argumento del comando `mount` especifica el sistema de archivos que se debe montar. El segundo argumento especifica el directorio como punto de montaje en la jerarquía de sistemas de archivos.

Puede montar el sistema de archivos de una de las siguientes maneras con el comando `mount`:

- Con el nombre del archivo del dispositivo en el directorio `/dev`.
- Con el UUID, un identificador único universal del dispositivo.

A continuación, identifique el dispositivo para montar, asegúrese de que exista el punto de montaje y monte el dispositivo en el punto de montaje.



nota

Si monta un sistema de archivos con el comando `mount` y luego reinicia su sistema, el sistema de archivos no se vuelve a montar automáticamente. El curso *Red Hat System Administration II* (RH134) explica cómo montar sistemas de archivos de forma persistente con el archivo `/etc/fstab`.

Identificación del dispositivo de bloque

Un dispositivo de almacenamiento conectable en funcionamiento, ya sea como unidad de disco duro (HDD) o dispositivo de estado sólido (SSD) o un portadiscos de almacenamiento USB, pueden conectarse a un puerto diferente cada vez que se conectan a un sistema. Use el comando `lsblk` para enumerar los detalles de un dispositivo de bloque especificado o todos los dispositivos disponibles.

```
[root@host ~]# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
vda    252:0    0  10G  0 disk
└─vda1 252:1    0   1M  0 part
└─vda2 252:2    0 200M  0 part /boot/efi
└─vda3 252:3    0 500M  0 part /boot
└─vda4 252:4    0  9.3G  0 part /
vdb    252:16   0   5G  0 disk
vdc    252:32   0   5G  0 disk
vdd    252:48   0   5G  0 disk
```

El tamaño de la partición ayuda a identificar el dispositivo cuando se desconoce el nombre de la partición. Por ejemplo, considerando la salida anterior, si el tamaño de la partición identificada es de 9.3 GB, monte la partición /dev/vda4.

Montar el sistema de archivos con el nombre de la partición

El siguiente ejemplo monta la partición /dev/vda4 en el punto de montaje /mnt/data.

```
[root@host ~]# mount /dev/vda4 /mnt/data
```

El directorio de punto de montaje debe existir antes de montar el sistema de archivos. El directorio /mnt existe de forma predeterminada para usarse como punto de montaje temporal.



Importante

Si un directorio que se usará como punto de montaje no está vacío, los archivos existentes se ocultarán y no se podrá acceder a ellos mientras se monte allí un sistema de archivos. Se podrá acceder a los archivos originales nuevamente después de desmontar el sistema de archivos montado.

El orden de detección de dispositivos y la denominación de dispositivos de almacenamiento pueden cambiar cuando se agregan o eliminan dispositivos en un sistema. Se recomienda usar un identificador de dispositivo que no cambie para montar sistemas de archivos de manera consistente.

Montar el sistema de archivos con la partición UUID

Un identificador estable que está asociado con un sistema de archivos es su identificador único universal (UUID). El UUID se almacena en el superbloque del sistema de archivos y se crea cuando se crea el sistema de archivos.

El comando `lsblk -fp` detalla la ruta completa del dispositivo, los UUID y los puntos de montajes, así como el tipo de sistema de archivos en la partición. El punto de montaje está en blanco cuando el sistema de archivos no está montado.

```
[root@host ~]# lsblk -fp
NAME      FSTYPE FSVER LABEL UUID                                     FSAVAIL FSUSE% MOUNTPOINTS
/dev/vda
└─/dev/vda1
└─/dev/vda2 vfat   FAT16    7B77-95E7          192.3M     4% /boot/efi
└─/dev/vda3 xfs    boot    2d67e6d0-...-1f091bf1  334.9M    32% /boot
└─/dev/vda4 xfs    root    efd314d0-...-ae98f652   7.7G    18% /
/dev/vdb
/dev/vdc
/dev/vdd
```

Monte el sistema de archivos por el UUID del sistema de archivos.

```
[root@host ~]# mount UUID="efd314d0-b56e-45db-bbb3-3f32ae98f652" /mnt/data
```

Montaje automático de dispositivos de almacenamiento extraíbles

Al usar el entorno de escritorio gráfico, el sistema monta automáticamente medios de almacenamiento extraíbles cuando se detecta la presencia de medios.

El dispositivo de almacenamiento extraíble se monta en la ubicación `/run/media/USERNAME/LABEL`. `USERNAME` es el nombre del usuario que inició sesión en el entorno gráfico. `LABEL` es un identificador, que generalmente es la etiqueta en los medios de almacenamiento.

Para desconectar de forma segura un dispositivo extraíble, primero desmonte manualmente todos los sistemas de archivos en el dispositivo.

Desmontaje de sistemas de archivos

Los procedimientos de apagado y reinicio del sistema desmontan todos los sistemas de archivos automáticamente. Todos los datos del sistema de archivos que se vacían en el dispositivo de almacenamiento para garantizar la integridad de los datos del sistema de archivos.



Advertencia

Los datos del sistema de archivos usan la memoria caché durante el funcionamiento normal. Debe desmontar los sistemas de archivos de una unidad extraíble antes de desconectar la unidad. El procedimiento de desmontaje vacía los datos en el disco antes de liberar la unidad.

Para desmontar un sistema de archivos, el comando `umount` usa el punto de montaje como argumento.

```
[root@host ~]# umount /mnt/data
```

No se puede desmontar cuando el sistema de archivos montado está en uso. Todos los procesos deben dejar de acceder a los datos en el punto de montaje para que el comando `umount` se ejecute correctamente.

En el siguiente ejemplo, el comando `umount` falla porque la shell usa el directorio `/mnt/data` como su directorio de trabajo actual y, por lo tanto, genera un mensaje de error.

```
[root@host ~]# cd /mnt/data
[root@host data]# umount /mnt/data
umount: /mnt/data: target is busy.
```

El comando `lsof` enumera todos los archivos abiertos y los procesos que acceden al sistema de archivos. La lista contribuye a identificar los procesos que actualmente impiden un correcto desmontaje del sistema de archivos.

```
[root@host data]# lsof /mnt/data
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
bash    1593 root cwd DIR 253,17      6  128 /mnt/data
lsof    2532 root cwd DIR 253,17     19  128 /mnt/data
lsof    2533 root cwd DIR 253,17     19  128 /mnt/data
```

Después de identificar los procesos, espere a que se completen o envíe la señal SIGTERM o SIGKILL para finalizarlos. En este caso, basta con cambiar el directorio en funcionamiento actual por un directorio fuera del punto de montaje.

```
[root@host data]# cd  
[root@host ~]# umount /mnt/data
```



Referencias

Páginas del manual: lsblk(8), mount(8), umount(8) y lsof(8).

► Ejercicio Guiado

Montaje y desmontaje de sistemas de archivos

En este ejercicio, practica montar y desmontar sistemas de archivos.

Resultados

- Identificar y montar un nuevo sistema de archivos en un punto de montaje especificado; luego, desmontarlo.

Antes De Comenzar

Con el usuario **student** en la máquina **workstation**, use el comando **lab** para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start fs-mount
```

Instrucciones

- 1. Inicie sesión en la máquina **servera** como el usuario **student** y cambie al usuario **root**.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

- 2. Se ha agregado una nueva partición con un sistema de archivos al disco **/dev/vdb** en la máquina **servera**. Monte la partición disponible recientemente mediante UUID en el punto de montaje **/mnt/part1**.

2.1. Cree el directorio **/mnt/part1**.

```
[root@servera ~]# mkdir /mnt/part1
```

2.2. Consulte el UUID del dispositivo **/dev/vdb1**.

NAME	FSTYPE	LABEL	UUID	MOUNTPOINT
/dev/vdb				
└─/dev/vdb1	xfs		a04c511a-b805-4ec2-981f-42d190fc9a65	

2.3. Monte el sistema de archivos mediante el uso del UUID en el directorio **/mnt/part1**. Use el UUID **/dev/vdb1** de la salida de comando anterior.

```
[root@servera ~]# mount \
UUID="a04c511a-b805-4ec2-981f-42d190fc9a65" /mnt/part1
```

2.4. Verifique que el dispositivo /dev/vdb1 esté montado en el directorio /mnt/part1.

```
[root@servera ~]# lsblk -fp /dev/vdb
NAME      FSTYPE LABEL UUID                                     MOUNTPOINT
/dev/vdb
└─/dev/vdb1 xfs    a04c511a-b805-4ec2-981f-42d190fc9a65 /mnt/part1
```

- 3. Cambie al directorio /mnt/part1 y cree el testdirsubdirectorio. Cree el archivo /mnt/part1/testdir/newmount.

3.1. Cambie al directorio /mnt/part1.

```
[root@servera ~]# cd /mnt/part1
```

3.2. Cree el directorio /mnt/part1/testdir.

```
[root@servera part1]# mkdir testdir
```

3.3. Cree el archivo /mnt/part1/testdir/newmount.

```
[root@servera part1]# touch testdir/newmount
```

- 4. Desmonte el sistema de archivos montado en el directorio /mnt/part1.

4.1. Desmonte el directorio /mnt/part1 mientras la shell está en el directorio /mnt/part1. El comando umount no puede desmontar el dispositivo.

```
[root@servera part1]# umount /mnt/part1
umount: /mnt/part1: target is busy.
```

4.2. Cambie el directorio actual en la shell al directorio /root.

```
[root@servera part1]# cd
[root@servera ~]#
```

4.3. Desmonte el directorio /mnt/part1.

```
[root@servera ~]# umount /mnt/part1
```

- 5. Regrese a la máquina workstation como el usuario student.

```
[root@servera ~]# exit  
logout  
[student@servera ~]$ exit  
logout  
Connection to servera closed.  
[student@workstation]$
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish fs-mount
```

Esto concluye la sección.

Adición de particiones, sistemas de archivos y montajes persistentes

Objetivos

Crear particiones de almacenamiento, formatearlas con sistemas de archivos y montarlas para su uso.

Discos de partición

La partición del disco divide un disco duro en varias *particiones* de almacenamiento lógico. Puede usar particiones para dividir el almacenamiento en función de diferentes requisitos y esta división proporciona numerosas ventajas:

- Limitar espacio disponible para aplicaciones o usuarios.
- Separar archivos de programa y de sistemas operativos de archivos de usuarios.
- Crear un área separada para el intercambio (swap) de memoria.
- 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

El esquema de partición *Master Boot Record* (MBR) es el estándar en los sistemas que ejecutan el firmware del BIOS. Este esquema soporta un máximo de cuatro particiones primarias. En sistemas Linux, con las particiones ampliadas y lógicas, puede crear un máximo de 15 particiones. Con un tamaño de partición de 32 bits, los discos que están particionados con MBR pueden tener un tamaño de hasta 2 TiB.



Figura 9.1: Particiones MBR del dispositivo de almacenamiento /dev/vdb

El límite de tamaño de disco y partición de 2 TiB ahora es una limitación común y restrictiva. En consecuencia, el esquema de MBR heredado es reemplazado por el esquema de partición *GUID Partition Table* (GPT).

Esquema de partición GPT

Para los sistemas que ejecutan el firmware de *Unified Extensible Firmware Interface* (UEFI), GPT es el estándar para la partición del disco y aborda las limitaciones del esquema de MBR. Un GPT proporciona un máximo de 128 particiones. El esquema GPT asigna 64 bits para direcciones de bloques lógicos, para soportar particiones y discos de hasta ocho zebabytes (ZiB) u ocho mil millones de tebibbytes (TiB).



Figura 9.2: Particiones GPT del dispositivo de almacenamiento /dev/vdb

La partición GPT ofrece características y ventajas adicionales sobre MBR. Un GPT usa un *identificador único global* (GUID) para identificar cada disco y partición. Un GPT hace que la tabla de particiones sea redundante, con el GPT principal en el cabezal del disco y un GPT secundario de respaldo en el extremo del disco. GPT usa la suma de comprobación para detectar errores en la tabla de particiones y el encabezado de GPT.

Administrar particiones

Un administrador puede usar un programa *editor de particiones* para cambiar particiones de un disco, como crear y eliminar particiones y cambiar los tipos de partición.



nota

¿Qué editor de particiones debería usar? Si bien los profesionales de TI tienen opiniones sólidas sobre las distinciones de funciones, cada editor aquí detallado realiza correctamente tareas comunes de preparación de discos.

- `fdisk` es uno de los favoritos históricos y ha soportado particiones GPT durante años.
- `gdisk` y otras variantes `fdisk` se crearon inicialmente para soportar GPT.
- `parted` y la librería `libparted` han sido el estándar de RHEL durante años.
- El instalador Anaconda continúa usando la librería `libparted`.
- `gnome-disk` es la herramienta gráfica predeterminada de GNOME, que reemplaza al upstream `gparted`.
- Casi todos los editores de la CLI son buenos para el scripting y `parted` fue diseñado para ello.

Los administradores pueden usar el editor de particiones `parted` tanto para el esquema de partición GPT como MBR. El comando `parted` toma el nombre del dispositivo de todo el disco como primer argumento seguido de subcomandos. En el siguiente ejemplo, se usa el subcomando `print` para visualizar la tabla de particiones en el disco `/dev/vda`.

```
[root@host ~]# parted /dev/vda print
Model: Virtio Block Device (virtblk)
Disk /dev/vda: 53.7GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Partition Flags:

Number  Start   End     Size    Type      File system  Flags
 1      1049kB  10.7GB  10.7GB  primary   xfs          boot
 2      10.7GB  53.7GB  42.9GB  primary   xfs
```

Use el comando `parted` sin un subcomando para abrir una sesión de partición interactiva.

```
[root@host ~]# parted /dev/vda
GNU Parted 3.4
Using /dev/vda
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted) print
Model: Virtio Block Device (virtblk)
Disk /dev/vda: 53.7GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

Number  Start   End     Size    Type      File system  Flags
 1      1049kB  10.7GB  10.7GB  primary   xfs          boot
 2      10.7GB  53.7GB  42.9GB  primary   xfs

(parted) quit
[root@host ~]#
```

De forma predeterminada, el comando `parted` muestra los tamaños en potencias de 10 (KB, MB, GB). Puede cambiar el tamaño de la unidad con el parámetro `unit`, que acepta los siguientes valores:

- **S** para sector
- **B** para byte
- **MiB**, **GiB** o **TiB** (potencias de 2)
- **MB**, **GB** o **TB** (potencias de 10)

```
[root@host ~]# parted /dev/vda unit s print
Model: Virtio Block Device (virtblk)
Disk /dev/vda: 104857600s
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

Number  Start     End      Size     Type      File system  Flags
 1      2048s    20971486s  20969439s  primary   xfs          boot
 2      20971520s 104857535s  83886016s  primary   xfs
```

Como se muestra en el ejemplo anterior, también puede especificar varios subcomandos (aquí, `unit` y `print`) en la misma línea.

Escritura de la tabla de particiones en un disco nuevo

Para particionar una nueva unidad, primero escriba una etiqueta de disco. La etiqueta del disco indica qué esquema de partición usar. Use `parted` para escribir una etiqueta de disco MBR o una etiqueta de disco GPT.

```
[root@host ~]# parted /dev/vdb mklabel msdos
[root@host ~]# parted /dev/vdb mklabel gpt
```

**Advertencia**

El subcomando `mklabel` borra la tabla de particiones existente. Use el subcomando `mklabel` cuando la intención sea volver a usar el disco sin tener en cuenta los datos existentes. Si una nueva etiqueta cambia los límites de la partición, todos los datos en los sistemas de archivos existentes se vuelven inaccesibles.

Creación de particiones de MBR

Las siguientes instrucciones crean una partición de disco MBR. Especifique el dispositivo de disco donde creará la partición.

Ejecute el comando `parted` y especifique el nombre del dispositivo de disco como un argumento, para comenzar en el modo interactivo. La sesión muestra (`parted`) como prompt de subcomando.

```
[root@host ~]# parted /dev/vdb
GNU Parted 3.4
Using /dev/vdb
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted)
```

Use el subcomando `mkpart` para crear una partición primaria o ampliada.

```
(parted) mkpart
Partition type? primary/extended? primary
```

**nota**

Si necesitan más de cuatro particiones en un disco particionado con MBR, cree tres particiones primarias y una partición ampliada. La partición ampliada sirve como contenedor dentro del cual se pueden crear varias particiones lógicas.

Indique el tipo de sistema de archivos que desea crear en la partición, como `xfs` o `ext4`. Este valor no crea el sistema de archivos, pero es solo una etiqueta de tipo de partición útil.

```
File system type? [ext2]? xfs
```

Para obtener la lista de los tipos de sistemas de archivos soportados, use el siguiente comando:

```
[root@host ~]# parted /dev/vdb help mkpart
...output omitted...
mkpart PART-TYPE [FS-TYPE] START END      make a partition

PART-TYPE is one of: primary, logical, extended
FS-TYPE is one of: udf, btrfs, nilfs2, ext4, ext3, ext2, f2fs, fat32, fat16,
hfsx, hfs+, hfs, jfs, swsusp, linux-swap(v1), linux-swap(v0), ntfs,
reiserfs, hp-ufs, sun-ufs, xfs, apfs2, apfs1, asfs, amufs5, amufs4, amufs3,
amufs2, amufs1, amufs0, amufs, affs7, affs6, affs5, affs4, affs3, affs2,
affs1, affs0, linux-swap, linux-swap(new), linux-swap(old)
```

```
'mkpart' makes a partition without creating a new file system on the
partition. FS-TYPE may be specified to set an appropriate partition
ID.
```

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

```
Start? 2048s
```

El sufijo s proporciona el valor en sectores o usa los sufijos MiB, GiB, TiB, MB, GB o TB. El comando `parted` toma de manera predeterminada el sufijo MB. El comando `parted` redondea los valores proporcionados para satisfacer las restricciones del disco.

Cuando se inicia el comando `parted`, recupera la topología del disco del dispositivo, como el tamaño del bloque físico del disco. El comando `parted` asegura que la posición de inicio que proporcione alinea correctamente la partición con la estructura del disco para optimizar el rendimiento. Si la posición de inicio genera una partición desalineada, el comando `parted` muestra una advertencia. Con la mayoría de los discos, un sector de inicio que es un múltiplo de 2048 es seguro.

Especifique el sector del disco donde debería terminar la nueva partición y salga de `parted`. Puede especificar el final como tamaño o como ubicación final.

```
End? 1000MB
(parted) quit
Information: You may need to update /etc/fstab.

[root@host ~]#
```

Al proporcionar la posición final, el comando `parted` actualiza la tabla de particiones en el disco con los detalles de la nueva partición.

Ejecute el comando `udevadm settle`. Este comando espera a que el sistema detecte la nueva partición y cree el archivo de dispositivo asociado en el directorio `/dev`. El prompt regresa cuando se realiza la tarea.

```
[root@host ~]# udevadm settle
```

Como alternativa al modo interactivo, puede crear una partición en un solo comando:

```
[root@host ~]# parted /dev/vdb mkpart primary xfs 2048s 1000MB
```

Creación de particiones GPT

El esquema GTP también usa el comando `parted` para crear particiones. Especifique el dispositivo de disco donde creará la partición.

Como usuario `root`, ejecute el comando `parted` y especifique el nombre del dispositivo de disco como un argumento.

```
[root@host ~]# parted /dev/vdb
GNU Parted 3.4
Using /dev/vdb
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted)
```

Use el subcomando `mkpart` para comenzar a crear la partición. Con el esquema GPT, cada partición recibe un nombre.

```
(parted) mkpart
Partition name? []? userdata
```

Indique el tipo de sistema de archivos que desea crear en la partición, como `xfs` o `ext4`. Este valor no crea el sistema de archivos, pero es una etiqueta de tipo de partición útil.

```
File system type? [ext2]? xfs
```

Especifique el sector del disco donde se iniciará la nueva partición.

```
Start? 2048s
```

Especifique el sector del disco donde debería terminar la nueva partición y salga de `parted`. Al proporcionar la posición final, el comando `parted` actualiza la tabla de particiones el GPT en el disco con los detalles de la nueva partición.

```
End? 1000MB
(parted) quit
Information: You may need to update /etc/fstab.

[root@host ~]#
```

Ejecute el comando `udevadm settle`. Este comando espera a que el sistema detecte la nueva partición y cree el archivo de dispositivo asociado en el directorio `/dev`. El prompt regresa cuando se realiza la tarea.

```
[root@host ~]# udevadm settle
```

Como alternativa al modo interactivo, puede crear una partición en un solo comando:

```
[root@host ~]# parted /dev/vdb mkpart userdata xfs 2048s 1000MB
```

Eliminación de particiones

Las siguientes instrucciones se aplican a los esquemas de partición MBR y GPT. Especifique el disco que contiene la partición que se eliminará.

Ejecute el comando `parted` con el dispositivo de disco como único argumento.

```
[root@host ~]# parted /dev/vdb
GNU Parted 3.4
Using /dev/vdb
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted)
```

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

```
(parted) print
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 5369MB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start   End     Size   File system  Name      Flags
 1       1049kB  1000MB  999MB  xfs          usersdata
```

Elimine la partición y salga de `parted`. El subcomando `rm` elimina inmediatamente la partición de la tabla de particiones en el disco.

```
(parted) rm 1
(parted) quit
Information: You may need to update /etc/fstab.

[root@host ~]#
```

Como alternativa al modo interactivo, puede eliminar una partición en un solo comando:

```
[root@host ~]# parted /dev/vdb rm 1
```

Creación de sistemas de archivos

Después de la creación de un dispositivo de bloque, el siguiente paso es agregarle un sistema de archivos. Red Hat Enterprise Linux soporta varios tipos de sistemas de archivos y XFS es el valor predeterminado recomendado.

Con el usuario `root`, use el comando `mkfs.xfs` para aplicar un sistema de archivos XFS a un dispositivo de bloque. Para un sistema de archivos ext4, use el comando `mkfs.ext4`.

```
[root@host ~]# mkfs.xfs /dev/vdb1
meta-data=/dev/vdb1              isize=512    agcount=4, agsize=60992 blks
                                =                      sectsz=512  attr=2, projid32bit=1
                                =                      crc=1        finobt=1, sparse=1, rmapbt=0
                                =                      reflink=1 bigtime=1 inobtcount=1
data     =                      bsize=4096   blocks=243968, imaxpct=25
                                =                      sunit=0     swidth=0 blks
naming  =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log          bsize=4096   blocks=1566, version=2
                                =                      sectsz=512  sunit=0 blks, lazy-count=1
realtime =none                  extsz=4096   blocks=0, rtextents=0
```

Montaje de sistemas de archivos

Después de agregar el sistema de archivos, el último paso es montar el sistema de archivos en un directorio en la estructura de directorios. Cuando monta un sistema de archivos en la jerarquía del directorio, las utilidades de espacio de usuarios pueden acceder o escribir archivos en el dispositivo.

Montaje manual de sistemas de archivos

Use el comando `mount` para conectar manualmente un dispositivo a una ubicación de directorio de *punto de montaje*. El comando `mount` requiere un dispositivo y un punto de montaje y puede incluir opciones de montaje del sistema de archivos. Las opciones del sistema de archivos personalizan el comportamiento del sistema de archivos.

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

También puede usar el comando `mount` para ver los sistemas de archivos montados actualmente, los puntos de montaje y sus opciones.

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

Montaje de manera persistente de sistemas de archivos

Montar manualmente un sistema de archivos es una buena manera de verificar que un dispositivo formateado sea accesible y funcione de la manera esperada. Sin embargo, cuando el servidor se reinicia, el sistema no vuelve a montar automáticamente el sistema de archivos.

Para configurar el sistema para que monte automáticamente el sistema de archivos durante el arranque del sistema, agregue una entrada al archivo `/etc/fstab`. Este archivo de configuración enumera los sistemas de archivos para montar en el arranque del sistema.

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

```
[root@host ~]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Thu Apr 5 12:05:19 2022
#
# 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.
#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#
UUID=a8063676-44dd-409a-b584-68be2c9f5570   /          xfs    defaults  0 0
UUID=7a20315d-ed8b-4e75-a5b6-24ff9e1f9838   /dbdata    xfs    defaults  0 0
```

El primer campo especifica el dispositivo. Este ejemplo usa un UUID para especificar el dispositivo. Los sistemas de archivos crean y almacenan el UUID en su superbloque de partición en el momento de la creación. O puede usar el archivo del dispositivo, como `/dev/vdb1`.

El segundo campo es el punto de montaje del directorio, desde el cual se podrá acceder al dispositivo de bloque en la estructura del directorio. El punto de montaje debe existir; de lo contrario, créelo con el comando `mkdir`.

El tercer campo contiene el tipo del sistema de archivos, como `xfs` o `ext4`.

El cuarto campo es la lista de opciones separada por comas para aplicar al dispositivo. `defaults` es un conjunto de opciones que se usan comúnmente. La página del manual `mount(8)` documenta las otras opciones disponibles.

El quinto campo es usado por el comando `dump` para hacer una copia de seguridad del dispositivo. Otras aplicaciones de copia de seguridad no suelen usar este campo.

El último campo, el campo de orden de `fsck`, determina si debería ejecutarse el comando `fsck` en el arranque del sistema para verificar que los sistemas de archivos estén limpios. El valor en este campo indica el orden en el que debe ejecutarse `fsck`. Para sistemas de archivos XFS, establezca este campo en `0` porque XFS no usa `fsck` para comprobar el estado de su sistema de archivos. Para sistemas de archivos `ext4`, configúrelo en `1` para el sistema de archivos `root` y en `2` para los otros sistemas de archivos `ext4`. Al usar esta notación, la utilidad `fsck` primero procesa el sistema de archivos `root` y, luego, verifica los sistemas de archivos en discos separados al mismo tiempo, y los sistemas de archivos en el mismo disco en secuencia.



nota

Si hay una entrada incorrecta en `/etc/fstab`, es posible que la máquina no pueda volver a arrancarse. Verifique que una entrada sea válida desmontando manualmente el nuevo sistema de archivos y, luego, use `mount /mountpoint` para leer el archivo `/etc/fstab` y vuelva a montar el sistema de archivos con las opciones de montaje de esa entrada. Si el comando `mount` arroja un error, corríjalo antes de volver a arrancar la máquina.

De manera alternativa, use el comando `findmnt --verify` para analizar el archivo `/etc/fstab` para la usabilidad de la partición.

Cuando agregue o elimine una entrada en el archivo `/etc/fstab`, ejecute el comando `systemctl daemon-reload`, o reinicie el servidor, para asegurar que el daemon `systemd` cargue y use la nueva configuración.

```
[root@host ~]# systemctl daemon-reload
```

Red Hat recomienda el uso de UUID para montar los sistemas de archivos de forma persistente, dado que los nombres de dispositivos 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, o que los discos se detecten en un orden diferente en un arranque del sistema. El nombre del archivo del dispositivo de bloque puede cambiar, pero el UUID permanece constante en el superbloque del sistema de archivos.

Use el comando `lsblk --fs` para escanear los dispositivos de bloque que están conectados a una máquina y recuperar los UUID del sistema de archivos.

```
[root@host ~]# lsblk --fs
NAME   FSTYPE  FSVER LABEL      UUID
vda
└─vda1
└─vda2 xfs    boot    49dd...75fdf  312M   37%   /boot
└─vda3 xfs    root    8a90...ce0da  4.8G   48%   /
```



Referencias

`info parted (GNU Parted User Manual)`

Páginas del manual: `parted(8)`, `mkfs(8)`, `mount(8)`, `lsblk(8)` y `fstab(5)`

Para obtener más información, consulte la guía *Configuring and Managing File Systems* en

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/managing_file_systems/index

► Ejercicio Guiado

Adición de particiones, sistemas de archivos y montajes persistentes

En este ejercicio, crea una partición en un nuevo dispositivo de almacenamiento, la formateará con un sistema de archivos XFS, la configurará para que se monte en el arranque y la montará para su uso.

Resultados

- Use `parted`, `mkfs.xfs` y otros comandos para crear una partición en un disco nuevo, formatearla y montarla de manera persistente.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start storage-partitions
```

Instrucciones

- 1. Inicie sesión en `servera` como el usuario `student` y cambie al usuario `root`.

```
student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

- 2. Cree una etiqueta de disco msdos en el dispositivo `/dev/vdb`.

```
[root@servera ~]# parted /dev/vdb mklabel msdos
Information: You may need to update /etc/fstab.
```

- 3. Agregue una partición principal de 1 GB. Para una correcta alineación, inicie la partición en el sector 2048. Establezca el tipo de sistema de archivo de la partición en XFS.

- 3.1. Use el modo interactivo `parted` para poder crear la partición.

```
[root@servera ~]# parted /dev/vdb
GNU Parted 3.4
Using /dev/vdb
Welcome to GNU Parted! Type 'help' to view a list of commands.
```

```
(parted) mkpart
Partition type? primary/extended? primary
File system type? [ext2]? xfs
Start? 2048s
End? 1001MB
(parted) quit
Information: You may need to update /etc/fstab.
```

Dado que la partición comienza en el sector 2048, el comando anterior establece la posición final en 1001 MB para obtener un tamaño de partición de 1000 MB (1 GB).

Como alternativa, puede realizar la misma operación con el siguiente comando no interactivo: `parted /dev/vdb mkpart primary xfs 2048s 1001 MB`

- 3.2. Verifique su trabajo enumerando las particiones en el dispositivo `/dev/vdb`.

```
[root@servera ~]# parted /dev/vdb print
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 5369MB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

Number  Start   End     Size    Type      File system  Flags
 1       1049kB  1001MB  1000MB  primary
```

- 3.3. Ejecute el comando `udevadm settle`. Este comando espera a que el sistema registre la nueva partición y regresa cuando finaliza.

```
[root@servera ~]# udevadm settle
```

- 4. Formatee la nueva partición con el sistema de archivos XFS.

```
[root@servera ~]# mkfs.xfs /dev/vdb1
meta-data=/dev/vdb1          isize=512    agcount=4, agsize=61056 blks
                           =           sectsz=512  attr=2, projid32bit=1
                           =           crc=1        finobt=1, sparse=1, rmapbt=0
                           =           reflink=1  bigtime=1 inobtcount=1
data          =           bsize=4096   blocks=244224, imaxpct=25
                           =           sunit=0      swidth=0 blks
naming        =version 2    bsize=4096   ascii-ci=0, ftype=1
log           =internal log bsize=4096   blocks=1566, version=2
                           =           sectsz=512  sunit=0 blks, lazy-count=1
realtime      =none         extsz=4096   blocks=0, rtextents=0
```

- 5. Configure el nuevo sistema de archivos para montarlo de forma persistente en el directorio `/archive`.

- 5.1. Cree el directorio `/archive`.

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

- 5.2. Descubra el UUID del dispositivo /dev/vdb1. El UUID en la salida probablemente sea diferente en su sistema.

```
[root@servera ~]# lsblk --fs /dev/vdb
NAME   FSTYPE FSVER LABEL UUID                                     FSAVAIL FSUSE%
MOUNTPOINTS
vdb
└─vdb1  xfs            881e856c-37b1-41e3-b009-ad526e46d987
```

- 5.3. Agregue una entrada al archivo /etc/fstab. Reemplace el UUID con el que descubrió en el paso anterior.

```
...output omitted...
UUID=881e856c-37b1-41e3-b009-ad526e46d987 /archive xfs defaults 0 0
```

- 5.4. Actualice el daemon systemd para que el sistema registre la nueva configuración del archivo /etc/fstab.

```
[root@servera ~]# systemctl daemon-reload
```

- 5.5. Monte el nuevo sistema de archivos con la nueva entrada en el archivo /etc/fstab.

```
[root@servera ~]# mount /archive
```

- 5.6. Verifique que el nuevo sistema de archivos esté montado en el directorio /archive.

```
[root@servera ~]# mount | grep /archive
/dev/vdb1 on /archive type xfs
(rw,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota)
```

- 6. Reinicie servera. Después de reiniciar el servidor, inicie sesión y verifique que el dispositivo /dev/vdb1 esté montado en el directorio /archive. Cuando finalice, cierre sesión de servera.

- 6.1. Reinicie servera.

```
[root@servera ~]# systemctl reboot
Connection to servera closed by remote host.
Connection to servera closed.
[student@workstation ~]$
```

- 6.2. Espere a que se reinicie servera e inicie sesión con el usuario student.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

- 6.3. Verifique que el dispositivo /dev/vdb1 esté montado en el directorio /archive.

```
[student@servera ~]$ mount | grep /archive
/dev/vdb1 on /archive type xfs
(rw,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota)
```

6.4. Regrese a la máquina **workstation** como el usuario **student**.

```
[student@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$
```

Finalizar

En la máquina **workstation**, cambie al directorio de inicio de usuario **student** y use el comando **lab** para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish storage-partitions
```

Esto concluye la sección.

Administración de espacio de intercambio (swap)

Objetivos

Crear y administrar espacios de intercambio (swap) para complementar la memoria física.

Conceptos de espacio de intercambio (swap)

Un *espacio de intercambio (swap)* es un área del disco bajo el control del subsistema de administración de memoria del kernel Linux. El kernel usa espacio de intercambio (swap) para complementar la memoria RAM del sistema al contener páginas inactivas en la memoria. La *memoria virtual* de un sistema abarca la memoria RAM del sistema y el espacio de intercambio (swap) combinados.

Cuando el uso de la memoria en un sistema supera un límite definido, el kernel busca en la memoria RAM páginas de memoria que están asignadas a los procesos, pero inactivas. El kernel escribe las páginas inactivas en el área de intercambio (swap) y, luego, reasigna la página RAM a otros procesos. Si un programa requiere acceso a una página en el disco, el kernel localiza otra página de memoria inactiva, la escribe en el disco y vuelve a convocar la página necesaria desde el área de intercambio (swap).

Dado que las áreas de intercambio (swap) residen en el disco, el intercambio es lento cuando se lo compara con la memoria RAM. Si bien el espacio de intercambio (swap) aumenta la memoria RAM del sistema, no debe considerar el espacio de intercambio como una solución sostenible para una RAM insuficiente para su carga de trabajo.

Cálculo del espacio de intercambio (swap)

Los administradores deben establecer el tamaño del espacio de intercambio (swap) en función de la carga de trabajo de memoria en el sistema. Los proveedores de aplicaciones a veces ofrecen recomendaciones para calcular el espacio de intercambio (swap). La siguiente tabla proporciona instrucciones basadas en la memoria física total.

Recomendaciones de memoria RAM y espacio de intercambio (swap)

RAM	Espacio de intercambio (swap)	Espacio de intercambio (swap) si se permite la hibernación
2 GB o menos	Dos veces la memoria RAM	Tres veces la memoria RAM
Entre 2 GB y 8 GB	Igual que la memoria RAM	Dos veces la memoria RAM
Entre 8 GB y 64 GB	Al menos 4 GB	1,5 veces la memoria RAM
Más de 64 GB	Al menos 4 GB	No se recomienda la hibernación.

La función de hibernación de los equipos portátiles y de escritorio usa el espacio de intercambio (swap) para guardar el contenido de la memoria RAM antes de apagar el sistema. Cuando vuelve a encender el sistema, el kernel restaura el contenido de la memoria RAM desde el espacio

de intercambio (swap) y no necesita un arranque completo. Para esos sistemas, el espacio de intercambio (swap) debe ser mayor que la cantidad de memoria RAM.

El artículo de la base de conocimiento en Referencias al final de esta sección brinda más orientación sobre el tamaño del espacio de intercambio (swap).

Creación de un espacio de intercambio (swap)

Para crear un espacio de intercambio (swap), debe realizar los siguientes pasos:

- Cree una partición con un tipo de sistema de archivos de `linux-swap`.
- Coloque una firma de intercambio (swap) en el dispositivo.

Creación de una partición de intercambio (swap)

Use el comando `parted` para crear una partición del tamaño adecuado y establezca su tipo de sistema de archivos en `linux-swap`. Anteriormente, las herramientas determinaban a partir del tipo de sistema de archivos de la partición si el dispositivo debía activarse; no obstante, eso ya no sucede. Si bien las utilidades ya no usan el tipo de sistema de archivos de la partición, los administradores pueden determinar rápidamente el propósito de la partición a partir de ese tipo.

En el siguiente ejemplo, se crea una partición de 256 MB.

```
[root@host ~]# parted /dev/vdb
GNU Parted 3.4
Using /dev/vdb
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted) print
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 5369MB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start   End     Size    File system  Name  Flags
 1      1049kB  1001MB  1000MB          data

(parted) mkpart
Partition name?  []? swap1
File system type? [ext2]? linux-swap
Start? 1001MB
End? 1257MB
(parted) print
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 5369MB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start   End     Size    File system  Name  Flags
 1      1049kB  1001MB  1000MB          data
 2      1001MB  1257MB  256MB   linux-swap(v1)  swap1

(parted) quit
```

```
Information: You may need to update /etc/fstab.
```

```
[root@host ~]#
```

Después de crear la partición, ejecute el comando `udevadm settle`. Este comando espera a que el sistema detecte la nueva partición y cree el archivo de dispositivo asociado en el directorio `/dev`. El comando regresa solo cuando finaliza.

```
[root@host ~]# udevadm settle
```

Formateo del espacio de intercambio (swap)

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

```
[root@host ~]# mkswap /dev/vdb2
Setting up swapspace version 1, size = 244 MiB (255848448 bytes)
no label, UUID=39e2667a-9458-42fe-9665-c5c854605881
```

Activación de un espacio de intercambio (swap)

Puede usar el comando `swapon` para activar un espacio de intercambio (swap) formateado.

Use `swapon` con el dispositivo como parámetro o use `swapon -a` para activar todos los espacios de intercambio (swap) detallados en el archivo `/etc/fstab`. Use los comandos `swapon --show` y `free` para inspeccionar los espacios de intercambio (swap) disponibles.

```
[root@host ~]# free
              total        used        free      shared  buff/cache   available
Mem:       1873036      134688      1536436          0        201912      1576044
Swap:          0          0          0
[root@host ~]# swapon /dev/vdb2
[root@host ~]# free
              total        used        free      shared  buff/cache   available
Mem:       1873036      135044      1536040          0        201952      1575680
Swap:      249852          0      249852
```

Puede desactivar un espacio de intercambio (swap) con el comando `swapoff`. Si el espacio de intercambio (swap) tiene páginas escritas, el comando `swapoff` intenta mover esas páginas a otros espacios de intercambio activos o volver a la memoria. Si el comando `swapoff` no puede escribir datos en otros lugares, falla con un error y el espacio de intercambio (swap) permanece activo.

Activación del espacio de intercambio (swap) de forma persistente

Cree una entrada en el archivo `/etc/fstab` para garantizar un espacio de intercambio (swap) activo en el arranque del sistema. En el siguiente ejemplo, se muestra una línea típica en el archivo `/etc/fstab` basada en el espacio de intercambio (swap) creado anteriormente.

```
UUID=39e2667a-9458-42fe-9665-c5c854605881 swap swap defaults 0 0
```

El ejemplo anterior usa el UUID como el primer campo. Cuando formatea el dispositivo, el comando `mkswap` muestra ese UUID. Si perdió la salida de `mkswap`, luego use el comando `lsblk - -fs`. Como alternativa, puede usar el nombre del dispositivo en el primer campo.

El segundo campo se reserva típicamente para el punto de montaje. Sin embargo, para dispositivos de intercambio (swap), que no son accesibles a través de la estructura del directorio, este campo toma el valor del marcador de posición swap. La página del manual `fstab(5)` usa un valor de marcador de posición de none; sin embargo, un valor de swap permite mensajes de error más informativos en el caso de que algo salga mal.

El tercer campo es el tipo de sistema de archivos. El tipo de sistemas de archivos para un espacio de intercambio (swap) es `swap`.

El cuarto campo es para opciones. El ejemplo usa la opción `defaults`. La opción `defaults` incluye la opción de montaje `auto`, que activa el espacio de intercambio (swap) automáticamente en el arranque del sistema.

Los dos campos finales son el indicador `dump` y el orden `fsck`. Los espacios de intercambio (swap) no requieren copias de seguridad ni revisión del sistema de archivos y, por lo tanto, estos campos deben establecerse en cero.

Cuando agregue o elimine una entrada en el archivo `/etc/fstab`, ejecute el comando `systemctl daemon-reload`, o reinicie el servidor, para `systemd` para registrar la nueva configuración.

```
[root@host ~]# systemctl daemon-reload
```

Configuración de la prioridad de espacio de intercambio (swap)

De forma predeterminada, el sistema usa espacios de intercambio (swap) en serie, lo que significa que el kernel usa el primer espacio de intercambio activado hasta que esté lleno y, luego, el kernel empieza a usar el segundo espacio de intercambio. En cambio, puede definir una prioridad para cada espacio de intercambio (swap) para forzar un orden particular.

Para establecer la prioridad, use la opción `pri` en el archivo `/etc/fstab`. El kernel usa el espacio de intercambio (swap) con la prioridad más alta primero. La prioridad predeterminada es -2.

En el siguiente ejemplo, se muestran tres espacios de intercambio (swap) definidos en el archivo `/etc/fstab`. El kernel usa la última entrada primero, ya que su prioridad se establece en 10.

Cuando ese espacio está lleno, usa la segunda entrada, ya que su prioridad está definida en 4. Por último, usa la primera entrada, que tiene una prioridad predeterminada de -2.

```
UUID=af30cbb0-3866-466a-825a-58889a49ef33 swap swap defaults 0 0
UUID=39e2667a-9458-42fe-9665-c5c854605881 swap swap pri=4 0 0
UUID=fbd7fa60-b781-44a8-961b-37ac3ef572bf swap swap pri=10 0 0
```

Use el comando `swapon - -show` para visualizar las prioridades de espacio de intercambio (swap).

Cuando los espacios de intercambio (swap) tienen la misma prioridad, el kernel los escribe con el método Round-Robin.



Referencias

Páginas del manual: `mkswap(8)`, `swapon(8)`, `swapoff(8)`, `mount(8)` y `parted(8)`

Base de conocimiento: ¿Cuál es el tamaño de intercambio (swap) recomendado para las plataformas Red Hat?

<https://access.redhat.com/solutions/15244>

► Ejercicio Guiado

Administración de espacio de intercambio (swap)

En este ejercicio, crea y formatea una partición para usar como espacio de intercambio (swap), la formateará como intercambio y la activará de forma persistente.

Resultados

- Crear una partición y un espacio de intercambio (swap) en un disco con el esquema de partición GPT.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start storage-swap
```

Instrucciones

- 1. Inicie sesión en `servera` como el usuario `student` y cambie al usuario `root`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

- 2. Inspeccione el disco `/dev/vdb`. El disco ya tiene una tabla de particiones y usa el esquema de partición GPT. Además, tiene una partición existente de 1 GB.

```
[root@servera ~]# parted /dev/vdb print
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 5369MB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Partition Flags:

Number  Start   End     Size    File system  Name  Flags
 1      1049kB  1001MB  1000MB          data
```

- 3. Agregue una nueva partición de 500 MB para usar como espacio de intercambio (swap). Establezca el tipo de partición en `linux-swap`.

- 3.1. Cree la partición `myswap`. Dado que el disco usa el esquema de partición GPT, debe asignarle un nombre a la partición. Observe que la posición inicial, 1001 MB, es el final de la primera partición existente. El comando `parted` se asegura de que la nueva partición siga inmediatamente a la anterior, sin ninguna brecha. Dado que la partición comienza en la posición 1001 MB, el comando establece la posición final en 1501 MB para obtener un tamaño de partición de 500 MB.

```
[root@servera ~]# parted /dev/vdb mkpart myswap linux-swap \
1001MB 1501MB
Information: You may need to update /etc/fstab.
```

- 3.2. Verifique su trabajo enumerando las particiones en el disco `/dev/vdb`. El tamaño de la nueva partición no es exactamente 500 MB. La diferencia de tamaño se debe a que el comando `parted` debe alinear la partición con el diseño del disco.

```
[root@servera ~]# parted /dev/vdb print
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 5369MB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start    End     Size   File system  Name    Flags
 1      1049kB  1001MB  1000MB          data
 2      1001MB  1501MB  499MB           myswap  swap
```

- 3.3. Ejecute el comando `udevadm settle`. Este comando espera a que el sistema registre la nueva partición y regresa cuando finaliza.

```
[root@servera ~]# udevadm settle
```

- 4. Inicialice la nueva partición como espacio de intercambio (swap).

```
[root@servera ~]# mkswap /dev/vdb2
Setting up swapspace version 1, size = 476 MiB (499118080 bytes)
no label, UUID=cb7f71ca-ee82-430e-ad4b-7dda12632328
```

- 5. Habilite el nuevo espacio de intercambio (swap).

- 5.1. Verifique que la creación e inicialización del espacio de intercambio (swap) no lo habilita aún para su uso.

```
[root@servera ~]# swapon --show
```

- 5.2. Habilite el nuevo espacio de intercambio (swap).

```
[root@servera ~]# swapon /dev/vdb2
```

- 5.3. Verifique que el nuevo espacio de intercambio (swap) ahora esté disponible.

```
[root@servera ~]# swapon --show
NAME      TYPE      SIZE USED PRIO
/dev/vdb2 partition 476M   0B   -2
```

- 5.4. Deshabilite el espacio de intercambio (swap).

```
[root@servera ~]# swapoff /dev/vdb2
```

- 5.5. Confirme que el espacio de intercambio (swap) está deshabilitado.

```
[root@servera ~]# swapon --show
```

► 6. Habilite el nuevo espacio de intercambio (swap) en el arranque del sistema.

- 6.1. Use el comando `lsblk` con la opción `--fs` para descubrir el UUID del dispositivo `/dev/vdb2`. El UUID en la salida será diferente en su sistema.

```
[root@servera ~]# lsblk --fs /dev/vdb2
NAME FSTYPE FSVER LABEL UUID                                     FSAVAIL FSUSE%
MOUNTPOINTS
vdb2 swap    1          762735cb-a52a-4345-9ed0-e3a68aa8bb97
```

- 6.2. Agregue una entrada al archivo `/etc/fstab`. En el siguiente comando, reemplace el UUID con el que descubrió en el paso anterior.

```
...output omitted...
UUID=762735cb-a52a-4345-9ed0-e3a68aa8bb97  swap  swap  defaults  0 0
```

- 6.3. Actualice el daemon `systemd` para que el sistema registre la nueva configuración del archivo `/etc/fstab`.

```
[root@servera ~]# systemctl daemon-reload
```

- 6.4. Habilite el espacio de intercambio (swap) usando la entrada en el archivo `/etc/fstab`.

```
[root@servera ~]# swapon -a
```

- 6.5. Verifique que el nuevo espacio de intercambio (swap) esté habilitado.

```
[root@servera ~]# swapon --show
NAME      TYPE      SIZE USED PRIO
/dev/vdb2 partition 476M   0B   -2
```

► 7. Reinicie la máquina `servera`. Después de reiniciar el servidor, inicie sesión y verifique que el espacio de intercambio (swap) esté habilitado. Cuando finalice, cierre sesión de `servera`.

- 7.1. Reinicie la máquina `servera`.

```
[root@servera ~]# systemctl reboot
Connection to servera closed by remote host.
Connection to servera closed.
[student@workstation ~]$
```

7.2. Espere a que se reinicie servera e inicie sesión con el usuario student.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

7.3. Verifique que el espacio de intercambio (swap) esté habilitado.

```
[student@servera ~]# swapon --show
NAME      TYPE      SIZE USED PRIO
/dev/vdb2  partition 476M   0B   -2
```

7.4. Regrese a la máquina workstation como el usuario student.

```
[student@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$
```

Finalizar

En la máquina **workstation**, cambie al directorio de inicio de usuario **student** y use el comando **lab** para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish storage-swap
```

Esto concluye la sección.

► Trabajo de laboratorio

Administración de almacenamiento básico

En este trabajo de laboratorio, crea varias particiones en un disco nuevo, formateará algunas con sistemas de archivos y las montará, y activará otras como espacios de intercambio (swap).

Resultados

- Visualizar y crear particiones con el comando `parted`.
- Crear sistemas de archivos en particiones y montarlos de forma persistente.
- Crear espacios de intercambio (swap) y activarlos en el arranque.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start storage-review
```

Instrucciones

1. La máquina `serverb` tiene varios discos sin usar. En el primer disco sin usar, cree una partición backup GPT de 2 GB. Dado que puede ser difícil establecer el tamaño exacto, un tamaño entre 1,8 GB y 2,2 GB es aceptable. Configure la partición backup para alojar un sistema de archivos XFS.
2. Formatee la partición backup de 2 GB con un sistema de archivos XFS y móntelo de manera persistente en el directorio `/backup`.
3. En el mismo disco, cree dos particiones GPT de 512 MB denominadas `swap1` y `swap2`. Un tamaño entre 460 MB y 564 MB es aceptable. Configure los tipos de sistemas de archivos de las particiones para alojar espacios de intercambio (swap).
4. Inicialice las dos particiones de 512 MiB como espacios de intercambio (swap) y configúrelas para que se activen en el arranque. Establezca el espacio de intercambio (swap) en la partición `swap2` para que se prefiera sobre el otro.
5. Para verificar su trabajo, reinicie la máquina `serverb`. Confirme que el sistema monta automáticamente la primera partición en el directorio `/backup`. Además, confirme que el sistema activa los dos espacios de intercambio (swap).

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade storage-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish storage-review
```

Esto concluye la sección.

► Solución

Administración de almacenamiento básico

En este trabajo de laboratorio, crea varias particiones en un disco nuevo, formateará algunas con sistemas de archivos y las montará, y activará otras como espacios de intercambio (swap).

Resultados

- Visualizar y crear particiones con el comando `parted`.
- Crear sistemas de archivos en particiones y montarlos de forma persistente.
- Crear espacios de intercambio (swap) y activarlos en el arranque.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start storage-review
```

Instrucciones

1. La máquina `serverb` tiene varios discos sin usar. En el primer disco sin usar, cree una partición backup GPT de 2 GB. Dado que puede ser difícil establecer el tamaño exacto, un tamaño entre 1,8 GB y 2,2 GB es aceptable. Configure la partición backup para alojar un sistema de archivos XFS.
 - 1.1. Inicie sesión en `serverb` como el usuario `student` y cambie al usuario `root`.

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
[student@serverb ~]$ sudo -i
[sudo] password for student: student
[root@serverb ~]#
```

- 1.2. Identifique los discos sin usar. El primer disco sin usar, `/dev/vdb`, no tiene particiones.

```
[root@serverb ~]# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
vda    252:0    0 10G  0 disk
└─vda1 252:1    0   1M  0 part
└─vda2 252:2    0 200M 0 part /boot/efi
└─vda3 252:3    0 500M 0 part /boot
└─vda4 252:4    0 9.3G 0 part /
```

```
vdb      252:16    0      5G  0 disk
vdc      252:32    0      5G  0 disk
vdd      252:48    0      5G  0 disk
```

- 1.3. Confirme que el disco /dev/vdb no tiene etiqueta.

```
[root@serverb ~]# parted /dev/vdb print
Error: /dev/vdb: unrecognised disk label
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 5369MB
Sector size (logical/physical): 512B/512B
Partition Table: unknown
Disk Flags:
```

- 1.4. Defina el esquema de partición GPT

```
[root@serverb ~]# parted /dev/vdb mklabel gpt
Information: You may need to update /etc/fstab.
```

- 1.5. Cree una partición backup de 2 GB con un tipo de sistema de archivos de xfs. Inicie la partición en el sector 2048.

```
[root@serverb ~]# parted /dev/vdb mkpart backup xfs 2048s 2GB
Information: You may need to update /etc/fstab.
```

- 1.6. Confirme la correcta creación de la partición backup.

```
[root@serverb ~]# parted /dev/vdb print
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 5369MB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start   End     Size   File system  Name     Flags
 1      1049kB  2000MB  1999MB          backup
```

- 1.7. Ejecute el comando udevadm settle. Este comando espera que el sistema detecte la nueva partición y cree el archivo de dispositivo /dev/vdb1.

```
[root@serverb ~]# udevadm settle
```

2. Formatee la partición backup de 2 GB con un sistema de archivos XFS y móntelo de manera persistente en el directorio /backup.

- 2.1. Formatee la partición /dev/vdb1.

```
[root@serverb ~]# mkfs.xfs /dev/vdb1
meta-data=/dev/vdb1              isize=512    agcount=4, agsize=121984 blks
                                =                      sectsz=512  attr=2, projid32bit=1
                                =                      crc=1       finobt=1, sparse=1, rmapbt=0
                                =                      reflink=1  bigtime=1 inobtcount=1
```

```

data      =          bsize=4096  blocks=487936, imaxpct=25
            =          sunit=0    swidth=0 blks
naming   =version 2  bsize=4096  ascii-ci=0, ftype=1
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

```

- 2.2. Cree el punto de montaje /backup.

```
[root@serverb ~]# mkdir /backup
```

- 2.3. Antes de agregar el nuevo sistema de archivos al archivo /etc/fstab, recupere su UUID. El UUID en su sistema podría ser diferente.

```

[root@serverb ~]# lsblk --fs /dev/vdb1
NAME FSTYPE FSVER LABEL UUID                                     FSAVAIL FSUSE%
MOUNTPOINTS
vdb1 xfs      f74ed805-b1fc-401a-a5ee-140f97c6757d

```

- 2.4. Edite el archivo /etc/fstab y defina el nuevo sistema de archivos.

```

[root@serverb ~]# vim /etc/fstab
...output omitted...
UUID=f74ed805-b1fc-401a-a5ee-140f97c6757d  /backup  xfs  defaults  0 0

```

- 2.5. Fuerce al daemon systemd para que vuelva a leer el archivo /etc/fstab.

```
[root@serverb ~]# systemctl daemon-reload
```

- 2.6. Monte manualmente el directorio /backup para verificar su trabajo. Confirme que el montaje sea correcto.

```

[root@serverb ~]# mount /backup
[root@serverb ~]# mount | grep /backup
/dev/vdb1 on /backup type xfs
(rw,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota)

```

3. En el mismo disco, cree dos particiones GPT de 512 MB denominadas swap1 y swap2. Un tamaño entre 460 MB y 564 MB es aceptable. Configure los tipos de sistemas de archivos de las particiones para alojar espacios de intercambio (swap).

- 3.1. Recupere la posición final de la primera partición visualizando la tabla de particiones actual en el disco /dev/vdb. En el siguiente paso, use ese valor como el inicio de la partición swap1.

```

[root@serverb ~]# parted /dev/vdb print
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 5369MB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

```

Number	Start	End	Size	File system	Name	Flags
1	1049kB	2000MB	1999MB	xfs		backup

- 3.2. Cree la primera partición swap1 de 512 MB. Establezca su tipo en linux-swap. Use la posición final de la primera partición como punto de partida. La posición final es 2000 MB + 512 MB = 2512 MB

```
[root@serverb ~]# parted /dev/vdb mkpart swap1 linux-swap 2000M 2512M
Information: You may need to update /etc/fstab.
```

- 3.3. Cree la segunda partición swap2 de 512 MB. Establezca su tipo en linux-swap. Use la posición final de la partición anterior como punto de partida: 2512M. La posición final es 2512 MB + 512 MB = 3024 MB

```
[root@serverb ~]# parted /dev/vdb mkpart swap2 linux-swap 2512M 3024M
Information: You may need to update /etc/fstab.
```

- 3.4. Visualice la tabla de particiones para verificar su trabajo.

```
[root@serverb ~]# parted /dev/vdb print
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 5369MB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start   End     Size    File system  Name     Flags
 1      1049kB  2000MB  1999MB  xfs        backup
 2      2000MB  2512MB  513MB   swap1      swap
 3      2512MB  3024MB  512MB   swap2      swap
```

- 3.5. Ejecute el comando udevadm settle. El comando espera que el sistema registre las nuevas particiones y cree los archivos de dispositivo.

```
[root@serverb ~]# udevadm settle
```

4. Inicialice las dos particiones de 512 MiB como espacios de intercambio (swap) y configúrelas para que se activen en el arranque. Establezca el espacio de intercambio (swap) en la partición swap2 para que se prefiera sobre el otro.

- 4.1. Use el comando mkswap para inicializar las particiones de intercambio (swap). Observe los UUID de los dos espacios de intercambio (swap), ya que usará esa información en el siguiente paso. Si borra la salida mkswap, use el comando lsblk --fs para recuperar los UUID.

```
[root@serverb ~]# mkswap /dev/vdb2
Setting up swap space version 1, size = 489 MiB (512749568 bytes)
no label, UUID=87976166-4697-47b7-86d1-73a02f0fc803
[root@serverb ~]# mkswap /dev/vdb3
Setting up swap space version 1, size = 488 MiB (511700992 bytes)
no label, UUID=4d9b847b-98e0-4d4e-9ef7-dfaaf736b942
```

- 4.2. Edite el archivo `/etc/fstab` y defina los nuevos espacios de intercambio (swap). Para configurar el espacio de intercambio (swap) en la partición swap2 para que se prefiera sobre la partición swap1, otórguele a la partición swap2 una mayor prioridad con la opción pri.

```
[root@serverb ~]# vim /etc/fstab
...output omitted...
UUID=a3665c6b-4bfb-49b6-a528-74e268b058dd  /backup xfs defaults 0 0
UUID=87976166-4697-47b7-86d1-73a02f0fc803  swap    swap  pri=10  0 0
UUID=4d9b847b-98e0-4d4e-9ef7-dfaaf736b942  swap    swap  pri=20  0 0
```

- 4.3. Fuerce al daemon `systemd` para que vuelva a leer el archivo `/etc/fstab`.

```
[root@serverb ~]# systemctl daemon-reload
```

- 4.4. Active los nuevos espacios de intercambio (swap). Verifique la correcta activación de los espacios de intercambio (swap).

```
[root@serverb ~]# swapon -a
[root@serverb ~]# swapon --show
NAME      TYPE      SIZE USED PRIO
/dev/vdb2  partition 489M   0B   10
/dev/vdb3  partition 488M   0B   20
```

5. Para verificar su trabajo, reinicie la máquina `serverb`. Confirme que el sistema monta automáticamente la primera partición en el directorio `/backup`. Además, confirme que el sistema activa los dos espacios de intercambio (swap).

- 5.1. Reinicie `serverb`.

```
[root@serverb ~]# systemctl reboot
Connection to serverb closed by remote host.
Connection to serverb closed.
[student@workstation ~]$
```

- 5.2. Espere a que se reinicie `serverb` y, luego, inicie sesión con el usuario `student`.

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
[student@serverb ~]$
```

- 5.3. Verifique que el sistema monta automáticamente la partición `/dev/vdb1` en el directorio `/backup`.

```
[student@serverb ~]$ mount | grep /backup
/dev/vdb1 on /backup type xfs (rw,relatime,seclabel,attr2,inode64,noquota)
```

- 5.4. Verifique que el sistema active ambos espacios de intercambio (swap).

```
[student@serverb ~]$ swapon --show
NAME      TYPE      SIZE USED PRIO
/dev/vdb2  partition 489M   0B   10
/dev/vdb3  partition 488M   0B   20
```

5.5. Regrese a la máquina `workstation` como el usuario `student`.

```
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@workstation ~]$
```

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade storage-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish storage-review
```

Esto concluye la sección.

Resumen

- El usuario `root` puede usar el comando `mount` para montar manualmente un sistema de archivos.
- El comando `parted` agrega, modifica y elimina particiones en discos con esquemas de partición MBR o GPT.
- El comando `mkfs.xfs` crea sistemas de archivos XFS en particiones de disco.
- El archivo `/etc/fstab` contiene dispositivos que deben montarse de forma persistente.
- El comando `mkswap` inicializa espacios de intercambio (swap).

capítulo 10

Administración de la pila (stack) de almacenamiento

Meta

Crear y administrar volúmenes lógicos que contengan sistemas de archivos o espacios de intercambio (swap) desde la línea de comandos.

Objetivos

- Describir los componentes y conceptos del administrador de volúmenes lógicos e implementar el almacenamiento de LVM y mostrar la información de los componentes de LVM.
- Analizar los múltiples componentes de almacenamiento que conforman las capas de la pila (stack) de almacenamiento.

Secciones

- Creación y ampliación de volúmenes lógicos (y ejercicio guiado)
- Administración de almacenamiento en capas (y ejercicio guiado)

Trabajo de laboratorio

Administración de la pila (stack) de almacenamiento

Creación y ampliación de volúmenes lógicos

Objetivos

Describir los componentes y conceptos del administrador de volúmenes lógicos e implementar el almacenamiento de LVM y mostrar la información de los componentes de LVM.

Descripción general del administrador de volúmenes lógicos

Use el sistema *administrador de volúmenes lógicos (LVM)* para crear volúmenes de almacenamiento lógico como una capa en el almacenamiento físico. Este sistema de almacenamiento proporciona una mayor flexibilidad que el uso de almacenamiento físico directamente. LVM oculta la configuración de almacenamiento de hardware del software y le permite cambiar el tamaño de los volúmenes sin detener las aplicaciones ni desmontar los sistemas de archivos. LVM proporciona herramientas completas de línea de comandos para administrar el almacenamiento.

Dispositivos físicos

Los volúmenes lógicos usan dispositivos físicos para almacenar datos. Estos dispositivos podrían ser particiones de discos, discos enteros, arreglos RAID o discos SAN. Debe inicializar el dispositivo como volumen físico LVM. Un volumen físico de LVM debe usar todo el dispositivo físico.

Volúmenes físicos (PV)

LVM usa el dispositivo físico subyacente como volumen físico de LVM. Las herramientas de LVM segmentan volúmenes físicos en *extensiones físicas (PE)* para formar pequeños conjuntos de datos que actúan como el bloque de almacenamiento más pequeño en un PV.

Grupos de volúmenes (VG)

Los grupos de volúmenes son conjuntos (pools) de almacenamiento conformados por uno o más PV. Se trata del equivalente funcional de un disco completo en comparación con el almacenamiento físico. Un PV solo puede ser asignado a un único VG. LVM establece el tamaño de la PE automáticamente, aunque es posible especificarlo. Un VG puede constar de espacio sin usar y de varios volúmenes lógicos.

Volúmenes lógicos (LV)

Los volúmenes lógicos se crean desde extensiones físicas libres en un VG y se proporcionan como el dispositivo de almacenamiento para aplicaciones, usuarios y sistemas operativos. Los LV son una colección de *extensiones lógicas (LE)*, que se asignan a extensiones físicas. De forma predeterminada, cada LE se asigna a una PE. La configuración de opciones de LV específicas cambia esta asignación; por ejemplo, la duplicación hace que cada LE se asigne a dos PE.

Flujo de trabajo del administrador de volúmenes lógicos

La creación del almacenamiento de LVM requiere la creación de estructuras en un flujo de trabajo lógico.

- Determine los dispositivos físicos usados para crear volúmenes físicos e inicialice estos dispositivos como volúmenes físicos de LVM.
- Cree un grupo de volúmenes a partir de varios volúmenes físicos.

- Cree los volúmenes lógicos del espacio disponible en el grupo de volúmenes.
- Formatee el volumen lógico con un sistema de archivos y móntelo o actívelo como espacio de intercambio (swap), o pase el volumen sin formato a una base de datos o servidor de almacenamiento para estructuras avanzadas.

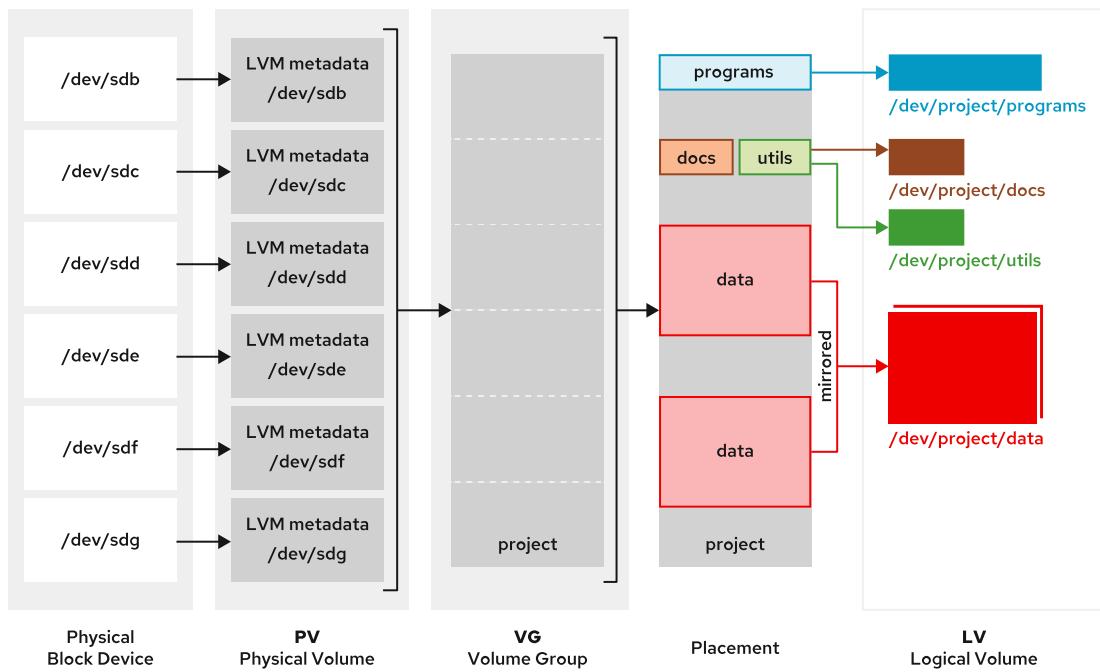


Figura 10.1: Flujo de trabajo del administrador de volúmenes lógicos

**nota**

Los ejemplos aquí usan un nombre de dispositivo /dev/vdb y sus particiones de almacenamiento. Los nombres de los dispositivos en el sistema en el aula pueden ser diferentes. Use los comandos `lsblk`, `blkid` o `cat /proc/partitions` para identificar los dispositivos en su sistema.

Creación del almacenamiento de LVM

La creación de un volumen lógico implica la creación de particiones de dispositivos físicos, volúmenes físicos y grupos de volúmenes. Después de crear un LV, formatee el volumen y móntelo para acceder a él como almacenamiento.

Preparación de dispositivos físicos

La partición es opcional cuando ya está presente. Use el comando `parted` para crear una nueva partición en el dispositivo físico. Establezca el dispositivo físico en el tipo de partición Linux LVM. Use el comando `udevadm settle` para registrar la nueva partición con el kernel.

```
[root@host ~]# parted /dev/vdb mklabel gpt mkpart primary 1MiB 769MiB
...output omitted...
[root@host ~]# parted /dev/vdb mkpart primary 770MiB 1026MiB
[root@host ~]# parted /dev/vdb set 1 lvm on
[root@host ~]# parted /dev/vdb set 2 lvm on
[root@host ~]# udevadm settle
```

Creación de volúmenes físicos

Use el comando `pvcreate` para etiquetar la partición física como volumen físico de LVM. Etiquete múltiples dispositivos al mismo tiempo al usar nombres de dispositivos delimitados por espacios como argumentos para el comando `pvcreate`. Este ejemplo etiqueta los dispositivos `/dev/vdb1` y `/dev/vdb2` como PV que están listos para crear grupos de volúmenes.

```
[root@host ~]# pvcreate /dev/vdb1 /dev/vdb2
Physical volume "/dev/vdb1" successfully created.
Physical volume "/dev/vdb2" successfully created.
Creating devices file /etc/lvm/devices/system.devices
```

Creación de un grupo de volúmenes

El comando `vgcreate` crea uno o más volúmenes físicos en un grupo de volúmenes. El primer comando es un nombre de grupo de volúmenes seguido de uno o más volúmenes físicos para asignar a este VG. Este ejemplo crea el VG `vg01` usando los PV `/dev/vdb1` y `/dev/vdb2`.

```
[root@host ~]# vgcreate vg01 /dev/vdb1 /dev/vdb2
Volume group "vg01" successfully created
```

Creación de un volumen lógico

El comando `lvcreate` crea un nuevo volumen lógico desde las PE disponibles en un grupo de volúmenes. Use el comando `lvcreate` para establecer el nombre y el tamaño del LV y el nombre del VG que contendrá este volumen lógico. Este ejemplo crea el LV `lv01` con un tamaño de 700 MiB en el VG `vg01`.

```
[root@host ~]# lvcreate -n lv01 -L 300M vg01
Logical volume "lv01" created.
```

Este comando podría fallar si el grupo de volúmenes no tiene suficientes extensiones físicas libres. El tamaño de LV se redondea al siguiente valor de tamaño de PE cuando el tamaño no coincide exactamente.

La opción `-L` del comando `lvcreate` requiere tamaños en bytes, mebibbytes (megabytes binarios, 1048576 bytes), gibibbytes (gigabytes binarios) o similar. La `-l` minúscula requiere tamaños especificados como una cantidad de extensiones físicas. Los siguientes comandos son dos opciones para crear el mismo LV con el mismo tamaño:

- `lvcreate -n lv01 -L 128M vg01`: crea un LV de 128 MiB, redondeado al siguiente PE.
- `lvcreate -n lv01 -l 32 vg01`: crea un LV de 32 PE a 4 MiB cada uno es 128 MiB.

Creación de un volumen lógico con desduplicación y compresión

RHEL 9 usa implementación de VDO de LVM para administrar volúmenes de VDO. Las herramientas de administración de VDO basadas en Python anteriores aún están disponibles, pero ya no son necesarias.

El *optimizador de datos virtual* (VDO) proporciona desduplicación de nivel de bloque en línea, compresión y aprovisionamiento ligero para el almacenamiento. Configure un volumen de VDO para usar hasta 256 TB de almacenamiento físico. Administrar VDO como un tipo de volumen

lógico (LV) de LVM, similar a los volúmenes con aprovisionamiento ligero de LVM. Un VDO de LVM está compuesto por dos volúmenes lógicos:

LV del conjunto (pool) de VDO

Este LV almacena, desduplica y comprime datos y establece el tamaño del volumen de VDO respaldado por el dispositivo físico. VDO se desduplica y comprime cada LV de VDO por separado porque cada LV de conjunto (pool) de VDO puede contener solo un LV de VDO.

LV de VDO

Un dispositivo virtual se aprovisiona sobre el LV del conjunto (pool) de VDO y establece el tamaño lógico del volumen de VDO que almacena los datos antes de que se produzca la desduplicación y la compresión.

VDO de LVM presenta el almacenamiento desduplicado como un volumen lógico regular (LV). El volumen de VDO puede formatearse con sistemas de archivos estándares, compartirse como un dispositivo de bloque o usarse para crear otras capas de almacenamiento, al igual que cualquier volumen lógico normal.

Para poder usar la desduplicación y compresión de VDO, instale los paquetes vdo y kmod-kvdo.

```
[root@host ~]# dnf install vdo kmod-kvdo
```

Verifique que el grupo de volúmenes de LVM seleccionado tenga suficiente capacidad de almacenamiento libre. Use el comando lvcreate con el parámetro --type vdo para crear un LV de VDO.

```
[root@host ~]# lvcreate --type vdo --name vdo-lv01 --size 5G vg01
Logical blocks defaulted to 523108 blocks.
The VDO volume can address 2 GB in 1 data slab.
It can grow to address at most 16 TB of physical storage in 8192 slabs.
If a larger maximum size might be needed, use bigger slabs.
Logical volume "vdo-lv01" created.
```

Creación de un sistema de archivos en volúmenes lógicos

Especifique el volumen lógico, ya sea usando el nombre tradicional /dev/vgname/lvname o el nombre del asignador de dispositivos del kernel /dev/mapper/_vgname_-lvname_.

Use el comando mkfs para crear un sistema de archivos en el nuevo volumen lógico.

```
[root@host ~]# mkfs -t xfs /dev/vg01/lv01
...output omitted...
```

Cree un punto de montaje con el comando mkdir.

```
[root@host ~]# mkdir /mnt/data
```

Para que el sistema de archivos esté disponible de manera persistente, agregue una entrada al archivo /etc/fstab.

```
/dev/vg01/lv01 /mnt/data xfs defaults 0 0
```

Monte el LV con el comando mount.

```
[root@host ~]# mount /mnt/data/
```

**nota**

Puede montar un volumen lógico por nombre o por UUID, ya que LVM analiza los PV en busca del UUID. Este comportamiento se realizó correctamente incluso cuando el VG se creó con un nombre, ya que el PV siempre contendrá un UUID.

Visualización del estado de los componentes de LVM

LVM proporciona varias utilidades para mostrar la información de estado de PV, VG y LV. Use los comandos `pvdisplay`, `vgdisplay` y `lvdisplay` para mostrar la información de estado de los componentes de LVM.

Los comandos `pvs`, `vgs` y `lvs` asociados se usan comúnmente y muestran un subconjunto de la información de estado, con una línea para cada entidad.

Visualización de la información de volumen físico

El comando `pvdisplay` muestra esta información acerca de PV. Use el comando sin argumentos para enumerar la información de todos los PV presentes en el sistema. Al proporcionar el nombre del PV como argumento para el comando, se muestra la información específica del PV.

```
[root@host ~]# pvdisplay /dev/vdb1
--- Physical volume ---
PV Name           /dev/vdb1          ①
VG Name           vg01              ②
PV Size           731.98 MiB / not usable 3.98 MiB ③
Allocatable       yes
PE Size           4.00 MiB          ④
Total PE          182
Free PE           107              ⑤
Allocated PE      75
PV UUID           zP0gD9-NxTV-Qtoi-yfQD-TGpL-0Yj0-wExh2N
```

- ① PV Name muestra el nombre del dispositivo.
- ② VG Name muestra el grupo de volúmenes donde se encuentra asignado el PV.
- ③ PV Size muestra el tamaño físico del PV, incluido todo el espacio no usable.
- ④ PE Size muestra el tamaño de la extensión física.
- ⑤ Free PE muestra el tamaño de PE disponible en el VG para crear nuevos LV o ampliar los LV existentes.

Visualización de la información de grupos de volúmenes

El comando `vgdisplay` muestra la información acerca de los grupos de volúmenes. Para mostrar información sobre todos los VG, use el comando sin argumentos. Proporcione el nombre del VG como argumento para enumerar la información específica del VG.

```
[root@host ~]# vgdisplay vg01
--- Volume group ---
VG Name          vg01          ①
System ID
Format           lvm2
Metadata Areas   2
Metadata Sequence No 2
VG Access        read/write
VG Status         resizable
MAX LV            0
Cur LV             1
Open LV            1
Max PV            0
Cur PV             2
Act PV             2
VG Size           1012.00 MiB      ②
PE Size            4.00 MiB
Total PE           253          ③
Alloc PE / Size   75 / 300.00 MiB
Free  PE / Size   178 / 712.00 MiB ④
VG UUID           jK5M1M-Yvlk-kxU2-bxmS-dNjQ-Bs3L-DRlJNc
```

- ① VG Name muestra el nombre del grupo de volúmenes.
- ② VG Size es el tamaño total del conjunto (pool) de almacenamiento disponible para la asignación de LV.
- ③ Total PE muestra el tamaño total de unidades de PE.
- ④ Free PE / Size muestra el espacio disponible en el VG para crear nuevos LV o ampliar los LV existentes.

Visualización de la información de volumen lógico

El comando `lvdisplay` muestra esta información acerca de volúmenes lógicos. Use el comando sin argumentos para enumerar la información de todos los LV. Proporcionar el nombre del LV como argumento muestra información específica del LV.

```
[root@host ~]# lvdisplay /dev/vg01/lv01
--- Logical volume ---
LV Path           /dev/vg01/lv01          ①
LV Name           lv01
VG Name           vg01          ②
LV UUID           FVmNel-u25R-dt3p-C5L6-VP2w-QRNP-scqrbq
LV Write Access   read/write
LV Creation host, time servera.lab.example.com, 2022-04-07 10:45:34 -0400
LV Status         available
# open            1
LV Size           300.00 MiB      ③
Current LE        75          ④
Segments          1
Allocation        inherit
```

```

Read ahead sectors      auto
 - currently set to     8192
 Block device           253:0

```

- ❶ LV Path muestra el nombre del dispositivo del LV.
- ❷ VG Name muestra el VG usado para crear este LV.
- ❸ LV Size muestra el tamaño total del LV. Use herramientas del sistema de archivos para determinar el espacio libre y usado para el LV.
- ❹ Current LE muestra el número de extensiones lógicas usadas por este LV.

Amplíe y reduzca el almacenamiento de LVM

Después de crear un volumen lógico, puede ampliar el volumen para ampliar el sistema de archivos. Es posible que necesite ampliar el PV o VG para aumentar la capacidad de almacenamiento del LV.

Ampliar el tamaño de un grupo de volúmenes

Es posible que deba agregar más espacio en disco para ampliar un VG. Puede agregar volúmenes físicos adicionales a un VG para ampliar su tamaño disponible.

Prepare el dispositivo físico y cree el volumen físico cuando no esté presente.

```

[root@host ~]# parted /dev/vdb mkpart primary 1072MiB 1648MiB
...output omitted...
[root@host ~]# parted /dev/vdb set 3 lvm on
...output omitted...
[root@host ~]# udevadm settle
[root@host ~]# pvcreate /dev/vdb3
Physical volume "/dev/vdb3" successfully created.

```

El comando `vgextend` agrega el nuevo PV al VG. Proporcione los nombres del VG y del PV como argumentos para el comando `vgextend`.

```

[root@host ~]# vgextend vg01 /dev/vdb3
Volume group "vg01" successfully extended

```

Este comando amplía el VG `vg01` al tamaño del PV `/dev/vdb3`.

Ampliación del volumen lógico

Un beneficio de usar volúmenes lógicos es aumentar su tamaño sin experimentar tiempo de inactividad. Agregue extensiones físicas libres al LV en el VG para ampliar su capacidad para ampliar el sistema de archivos del LV. Use el comando `vfdisplay` para confirmar que el grupo de volúmenes tenga suficiente espacio libre para la extensión del LV.

Use el comando `lvextend` para ampliar el LV.

```
[root@host ~]# lvextend -L +500M /dev/vg01/lv01
  Size of logical volume vg01/lv01 changed from 300.00 MiB (75 extents) to 800.00
  MiB (200 extents).
  Logical volume vg01/lv01 successfully resized.
```

Esto aumenta el tamaño del volumen lógico `lv01` en 500 MiB. El signo más (+) delante del tamaño significa que desea agregar este valor al tamaño existente; de lo contrario, sin el signo más, el valor define el tamaño final del LV.

El comando `lvextend` usa diferentes métodos para especificar el tamaño. La opción `-l` del comando `lvextend` espera el número de PE como argumento. La opción `-L` del comando `lvextend` espera tamaños en bytes, mebibbytes, gibibbytes y similares.

Ampliación de un sistema de archivos XFS al tamaño de volumen lógico

El comando `xfs_growfs` ayuda a ampliar el sistema de archivos para que ocupe el LV ampliado. El sistema de archivos de destino se debe montar antes de usar el comando `xfs_growfs`. Puede seguir usando el sistema de archivos mientras se cambia el tamaño.

```
[root@host ~]# xfs_growfs /mnt/data/
...output omitted...
data blocks changed from 76800 to 204800
```



Importante

Ejecute siempre el comando `xfs_growfs` después de ejecutar el comando `lvextend`. Use la opción `-r` del comando `lvextend` para ejecutar los dos pasos consecutivamente. Después de ampliar el LV, cambia el tamaño del sistema de archivos con el comando `fsadm`. Esta opción soporta varios otros sistemas de archivos.

Ampliación de un sistema de archivos EXT4 al tamaño de volumen lógico

Los pasos para ampliar el LV con el sistema de archivos `ext4` son los mismos para LV con el sistema de archivos `XFS`, excepto por el paso para cambiar el tamaño del sistema de archivos.

El comando `resize2fs` amplía el sistema de archivos para ocupar el nuevo LV ampliado. Puede seguir usando el sistema de archivos mientras se cambia el tamaño.

```
[root@host ~]# resize2fs /dev/vg01/lv01
resize2fs 1.46.5 (30-Dec-2021)
Resizing the filesystem on /dev/vg01/lv01 to 256000 (4k) blocks.
The filesystem on /dev/vg01/lv01 is now 256000 (4k) blocks long.
```

La principal diferencia entre `xfs_growfs` y `resize2fs` es el argumento que se pasó para identificar el sistema de archivos. El comando `xfs_growfs` toma el punto de montaje como argumento y el comando `resize2fs` toma el nombre del LV como argumento. El comando `xfs_growfs` solo soporta un cambio de tamaño en línea, mientras que el comando `resize2fs` soporta el cambio de tamaño en línea y sin conexión. Puede cambiar el tamaño de un sistema de

archivos ext4 hacia arriba o hacia abajo, pero solo puede cambiar el tamaño de un sistema de archivos XFS.

Ampliación de volúmenes lógicos del espacio de intercambio (swap)

Puede ampliar los LV usados como espacio de intercambio (swap); sin embargo, el proceso difiere de ampliar el sistema de archivos ext4 o XFS. Los volúmenes lógicos usados como espacio de intercambio (swap) se deben desconectar para ampliarse.

Use el comando `swapoff` para desactivar el espacio de intercambio (swap) en el LV.

```
[root@host ~]# swapoff -v /dev/vg01/swap
swapoff /dev/vg01/swap
```

Use el comando `lvextend` para ampliar el LV.

```
[root@host ~]# lvextend -L +300M /dev/vg01/swap
  Size of logical volume vg01/swap changed from 500.00 MiB (125 extents) to 800.00
  MiB (200 extents).
  Logical volume vg01/swap successfully resized.
```

Use el comando `mkswap` para formatear el LV como espacio de intercambio (swap).

```
[root@host ~]# mkswap /dev/vg01/swap
mkswap: /dev/vg01/swap: warning: wiping old swap signature.
Setting up swap space version 1, size = 800 MiB (838856704 bytes)
no label, UUID=25b4d602-6180-4b1c-974e-7f40634ad660
```

Use el comando `swapon` para activar el espacio de intercambio (swap) en el LV.

```
[root@host ~]# swapon /dev/vg01/swap
```

Reducción del almacenamiento del grupo de volúmenes

Reducir un VG implica eliminar el PV no usado del VG. El comando `pvmove` mueve datos de extensiones en un PV a extensiones en otro PV con suficientes extensiones libres en el mismo VG. Puede continuar usando el LV desde el mismo VG mientras reduce. Use la opción `-A` del comando `pvmove` para hacer una copia de seguridad automática de los metadatos del VG después de un cambio. Esta opción usa el comando `vfcfgbackup` para hacer una copia de seguridad de los metadatos automáticamente.

```
[root@host ~]# pvmove /dev/vdb3
```



Advertencia

Antes de usar el comando `pvmove`, realice una copia de seguridad de los datos almacenados en todos los LV en el VG. Una pérdida de energía inesperada durante la operación puede dejar al VG en un estado inconsistente que podría causar una pérdida de datos en los LV.

Use el comando `vgreduce` para eliminar un PV de un VG.

```
[root@host ~]# vgreduce vg01 /dev/vdb3
Removed "/dev/vdb3" from volume group "vg01"
```



Importante

Los sistemas de archivos GFS2 y XFS no soportan la reducción, por lo que no puede reducir el tamaño de un LV.

Eliminar almacenamiento de LVM

Use los comandos `lvremove`, `vgremove` y `pvremove` para eliminar un componente de LVM que ya no es necesario.

Preparación del sistema de archivos

Traslade todos los datos que se deben conservar a otro sistema de archivos. Use el comando `umount` para desmontar el sistema de archivos y, luego, eliminar cualquier entrada de `/etc/fstab` asociada a este sistema de archivos.

```
[root@host ~]# umount /mnt/data
```



Advertencia

Al eliminar un volumen lógico, se destruyen todos los datos almacenados en este. Realice una copia de seguridad de los datos o trasládelos **antes** de eliminar el volumen lógico.

Eliminación del volumen lógico

Use el comando `lvremove DEVICE-NAME` para eliminar un volumen lógico que ya no es necesario. Desmonte el sistema de archivos del LV antes de ejecutar este comando. El comando solicita confirmación antes de eliminar el LV.

```
[root@host ~]# lvremove /dev/vg01/lv01
Do you really want to remove active logical volume vg01/lv01? [y/n]: y
Logical volume "lv01" successfully removed.
```

Las extensiones físicas del LV se liberan y están disponibles para ser asignadas a LV existentes o nuevos en el grupo de volúmenes.

Eliminación del grupo de volúmenes

Use el comando `vgremove VG-NAME` para eliminar un grupo de volúmenes que ya no es necesario.

```
[root@host ~]# vgremove vg01
Volume group "vg01" successfully removed
```

Los volúmenes físicos del VG se liberan y están disponibles para ser asignados a VG existentes o nuevos en el sistema.

Eliminación de volúmenes lógicos

Use el comando `pvremove` 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. Este comando elimina los metadatos del PV de la partición (o disco). Ahora, la partición está libre para una nueva asignación o para ser formateada.

```
[root@host ~]# pvremove /dev/vdb1 /dev/vdb2
  Labels on physical volume "/dev/vdb1" successfully wiped.
  Labels on physical volume "/dev/vdb2" successfully wiped.
```



Referencias

Páginas del manual: `fdisk(8)`, `gdisk(8)`, `parted(8)`, `partprobe(8)`, `lvm(8)`, `pvcREATE(8)`, `vgCREATE(8)`, `lvCREATE(8)`, `mkfs(8)`, `pVDISPLAY(8)`, `VGDISPLAY(8)`, `lVDISPLAY(8)`, `vgEXTEND(8)`, `lvEXTEND(8)`, `xFS_gROWFS(8)`, `RESIZE2FS(8)`, `SWAPOFF(8)`, `MKSWAP(8)`, `SWAPON(8)`, `PVMOVE(8)`, `VGCFGBACKUP(8)`, `VGREDUCE(8)`, `LVREMOVE(8)`, `VGREMOVE(8)`, `PVREMOVE(8)`

Para obtener más información, consulte *Configuring and Managing Logical Volumes* en

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/configuring_and_managing_logical_volumes/index

► Ejercicio Guiado

Creación y ampliación de volúmenes lógicos

En este trabajo de laboratorio, crea y amplía un volumen físico, un grupo de volúmenes, un volumen lógico y un sistema de archivos XFS. También monta de forma persistente el sistema de archivos de volúmenes lógicos.

Resultados

- Crear volúmenes físicos, grupos de volúmenes y volúmenes lógicos con herramientas de LVM.
- Crear nuevos sistemas de archivos en volúmenes lógicos y montarlos de manera persistente.
- Ampliar el grupo de volúmenes para incluir un volumen físico adicional.
- Cambiar el tamaño del volumen lógico mientras el sistema de archivos aún está montado y en uso.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start lvm-manage
```

Instrucciones

- 1. Inicie sesión en la máquina `servera` como el usuario `student` y cambie al usuario `root`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

- 2. Cree la partición del dispositivo físico en el dispositivo de almacenamiento `/dev/vdb`.

- 2.1. Cree dos particiones de 256 MiB cada una y configúrelas con el tipo Linux LVM. Use `first` y `second` como nombres para estas particiones.

```
[root@servera ~]# parted /dev/vdb mklabel gpt
[root@servera ~]# parted /dev/vdb mkpart first 1MiB 258MiB
[root@servera ~]# parted /dev/vdb set 1 lvm on
[root@servera ~]# parted /dev/vdb mkpart second 258MiB 514MiB
[root@servera ~]# parted /dev/vdb set 2 lvm on
```

- 2.2. Registre las nuevas particiones con el kernel.

```
[root@servera ~]# udevadm settle
```

- 2.3. Enumere las particiones en el dispositivo de almacenamiento `/dev/vdb`. En la columna `Number`, los valores 1 y 2 corresponden a las particiones del dispositivo `/dev/vdb1` y `/dev/vdb2`. La columna `Flags` indica el tipo de partición.

```
[root@servera ~]# parted /dev/vdb print
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 5369MB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start   End     Size    File system  Name     Flags
 1      1049kB  271MB   269MB   first      lvm
 2      271MB   539MB   268MB   second      lvm
```

- ▶ 3. Etiquete las dos nuevas particiones como volúmenes físicos.

```
[root@servera ~]# pvcreate /dev/vdb1 /dev/vdb2
Physical volume "/dev/vdb1" successfully created.
Physical volume "/dev/vdb2" successfully created.
Creating devices file /etc/lvm/devices/system.devices
```

- ▶ 4. Cree el grupo de volúmenes `servera_group` con los dos nuevos PV.

```
[root@servera ~]# vgcreate servera_group /dev/vdb1 /dev/vdb2
Volume group "servera_group" successfully created
```

- ▶ 5. Cree el volumen lógico `servera_volume` con un tamaño de 400 MiB. Este comando crea el LV `/dev/servera_group/servera_volume` sin un sistema de archivos.

```
[root@servera ~]# lvcreate -n servera_volume -L 400M servera_group
Logical volume "servera_volume" created.
```

- ▶ 6. Formatee el LV recién creado y móntelo de forma persistente.

- 6.1. Formatee el nuevo LV `servera_volume` con el sistema de archivos XFS.

```
[root@servera ~]# mkfs -t xfs /dev/servera_group/servera_volume
...output omitted...
```

- 6.2. Cree el directorio `/data` como punto de montaje.

```
[root@servera ~]# mkdir /data
```

- 6.3. Para montar de manera persistente el sistema de archivos creado recientemente, agregue el siguiente contenido en el archivo `/etc/fstab`.

```
/dev/servera_group/servera_volume /data xfs defaults 0 0
```

6.4. Monte el LV servera_volume.

```
[root@servera ~]# mount /data
```

- 7. Verifique que se pueda acceder al sistema de archivos montado y visualice la información de estado del LVM.

7.1. Verifique que pueda copiar archivos en el directorio /data.

```
[root@servera ~]# cp -a /etc/*.* /data
[root@servera ~]# ls /data | wc -l
32
```

- 7.2. Vea la información de estado de PV. La salida muestra que el PV usa el VG **servera_group**. El PV tiene un tamaño de 256 MiB y el tamaño de la extensión física de 4 MiB.

Hay 63 PE, con 27 PE disponibles para la asignación y 36 PE actualmente asignadas al LV. Al calcular el tamaño en MiB:

- Total de 252 MiB (63 PE x 4 MiB).
- 108 MiB libres (27 PE x 4 MiB)
- 144 MiB asignados (36 PE x 4 MiB)

```
[root@servera ~]# pvdisplay /dev/vdb2
--- Physical volume ---
PV Name           /dev/vdb2
VG Name           servera_group
PV Size          256.00 MiB / not usable 4.00 MiB
Allocatable       yes
PE Size          4.00 MiB
Total PE         63
Free PE          27
Allocated PE     36
PV UUID          FKKFYJ-wJiR-1jt2-sfy3-yjPy-TyLN-LG92jj
```

- 7.3. Vea la información de estado de PV del VG **servera_group**. La salida muestra el VG de 508 MiB con el PE de 4 MiB. El tamaño disponible del VG es 108 MiB.

```
[root@servera ~]# vgdisplay servera_group
--- Volume group ---
VG Name           servera_group
System ID
Format           lvm2
Metadata Areas   2
Metadata Sequence No 2
VG Access        read/write
VG Status        resizable
MAX LV
Cur LV
```

```

Open LV          1
Max PV          0
Cur PV          2
Act PV          2
VG Size        508.00 MiB
PE Size         4.00 MiB
Total PE        127
Alloc PE / Size 100 / 400.00 MiB
Free PE / Size  27 / 108.00 MiB
VG UUID        g0ahyT-90J5-iGic-nnb5-G6T9-tLdK-dX8c9M

```

- 7.4. Vea la información de estado del LV `servera_volume`. La salida muestra el nombre de VG usado para crear el LV. También muestra el LV de 400 MiB y el LE de 100.

```

[root@servera ~]# lvdisplay /dev/servera_group/servera_volume
--- Logical volume ---
LV Path          /dev/servera_group/servera_volume
LV Name          servera_volume
VG Name          servera_group
LV UUID          93MfUt-esgT-B5HM-r1p5-DVZH-n5cn-J5e2tw
LV Write Access   read/write
LV Creation host, time servera.lab.example.com, 2022-04-11 03:25:12 -0400
LV Status        available
# open           1
LV Size          400.00 MiB
Current LE       100
Segments         2
Allocation       inherit
Read ahead sectors auto
- currently set to 8192
Block device     253:0

```

- 7.5. Vea el espacio libre en disco en unidades legibles por humanos. La salida muestra el tamaño total de 395 MiB con el tamaño disponible de 372 MiB.

```

[root@servera ~]# df -h /data
Filesystem           Size  Used Avail Use% Mounted on
/dev/mapper/servera_group-servera_volume  395M   24M  372M   6% /data

```

► 8. Cree los recursos físicos en el dispositivo de almacenamiento `/dev/vdb`.

- 8.1. Cree una partición adicional de 512 MiB y configúrela con el tipo Linux LVM. Use `third` como el nombre para esta partición.

```

[root@servera ~]# parted /dev/vdb mkpart third 514MiB 1026MiB
[root@servera ~]# parted /dev/vdb set 3 lvm on

```

- 8.2. Registre la nueva partición con el kernel.

```
[root@servera ~]# udevadm settle
```

- 8.3. Agregue la nueva partición como un PV.

```
[root@servera ~]# pvcreate /dev/vdb3
Physical volume "/dev/vdb3" successfully created.
```

- ▶ 9. Con el espacio en disco creado recientemente, amplíe el sistema de archivos en `servera_volume` para que tenga un tamaño total de 700 MiB.

9.1. Extienda el VG `servera_group` con el nuevo PV `/dev/vdb3`.

```
[root@servera ~]# vgextend servera_group /dev/vdb3
Volume group "servera_group" successfully extended
```

9.2. Amplíe el LV `servera_volume` existente a 700 MiB.

```
[root@servera ~]# lvextend -L 700M /dev/servera_group/servera_volume
Size of logical volume servera_group/servera_volume changed from 400.00 MiB (100
extents) to 700.00 MiB (175 extents).
Logical volume servera_group/servera_volume successfully resized.
```

9.3. Amplíe el sistema de archivos XFS con espacio libre del LV.

```
[root@servera ~]# xfs_growfs /data
...output omitted...
data blocks changed from 102400 to 179200
```

- ▶ 10. Verifique que el tamaño del LV se haya ampliado y que el contenido aún esté presente en el volumen.

10.1. Verifique el tamaño del LV extendido con el comando `lvdisplay`.

```
[root@servera ~]# lvdisplay /dev/servera_group/servera_volume
--- Logical volume ---
LV Path          /dev/servera_group/servera_volume
LV Name          servera_volume
VG Name          servera_group
LV UUID          mLQhsD-hyL0-KC2B-2nug-o2Nc-0zns-Q428fK
LV Write Access  read/write
LV Creation host, time servera.lab.example.com, 2022-04-12 06:04:12 -0400
LV Status        available
# open           1
LV Size          700.00 MiB
Current LE       175
Segments         3
Allocation       inherit
Read ahead sectors auto
- currently set to 8192
Block device     253:0
```

10.2. Verifique el tamaño del nuevo sistema de archivos. Verifique que los archivos copiados anteriormente aún estén presentes.

```
[root@servera ~]# df -h /data
Filesystem                      Size  Used Avail Use% Mounted on
/dev/mapper/servera_group-servera_volume  695M   26M  670M   4% /data
[root@servera ~]# ls /data | wc -l
32
```

- 11. Regrese a la máquina **workstation** como el usuario **student**.

```
[root@servera ~]# exit
logout
[student@servera ~]$ exit
logout
Connection to servera closed.
```

Finalizar

En la máquina **workstation**, cambie al directorio de inicio de usuario **student** y use el comando **lab** para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish lvm-manage
```

Esto concluye la sección.

Administración de almacenamiento en capas

Objetivos

Analizar los múltiples componentes de almacenamiento que conforman las capas de la pila (stack) de almacenamiento.

Pila (stack) de almacenamiento

El almacenamiento en RHEL está compuesto por varias capas de controladores, administradores y utilidades que son maduras, estables y están llenas de características modernas. La administración del almacenamiento requiere estar familiarizado con los componentes de la pila (stack) y reconocer que la configuración del almacenamiento afecta el proceso de arranque, el rendimiento de la aplicación y la capacidad de proporcionar las funciones de almacenamiento necesarias para casos de uso específicos de la aplicación.

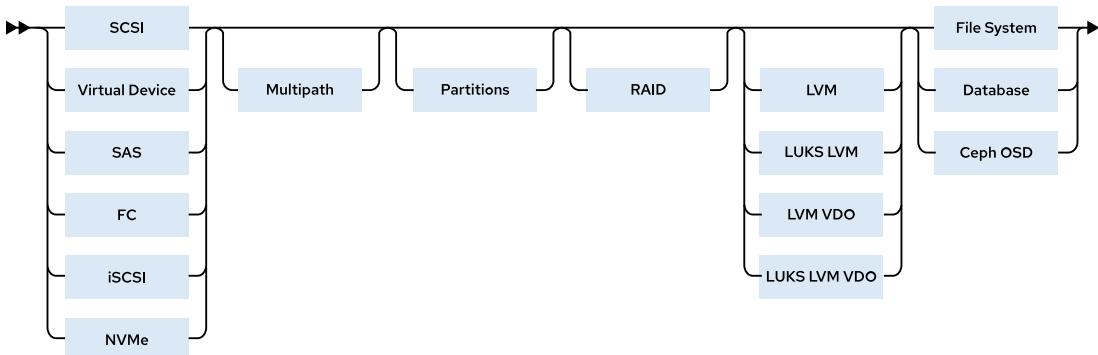


Figura 10.2: Pila (stack) de almacenamiento

Las secciones anteriores de los cursos Red Hat System Administration han presentado los sistemas de archivos XFS, el uso compartido de almacenamiento de red, la partición y el administrador de volúmenes lógicos. En esta sección, se presenta una descripción general de la pila (stack) de almacenamiento de RHEL de abajo hacia arriba y se presenta cada capa.

Esta sección también abarca Stratis, el daemon que unifica, configura y monitorea los componentes de la pila (stack) de almacenamiento RHEL subyacentes, y proporciona administración de almacenamiento local automatizada desde la CLI o desde la consola web de RHEL.

Dispositivo de bloque

Los dispositivos de bloque se encuentran en la parte inferior de la pila (stack) de almacenamiento y presentan un protocolo de dispositivo estable y uniforme que permite que prácticamente cualquier dispositivo de bloque se incluya de forma transparente en una configuración de almacenamiento RHEL. En la actualidad, se accede a la mayoría de los dispositivos de bloque a través del controlador de dispositivos SCSI de RHEL y aparecen como un dispositivo SCSI, incluidos los discos duros ATA heredados, los dispositivos de estado sólido y los adaptadores de bus de host (HBA) empresariales comunes. RHEL también soporta iSCSI, canal de fibra a través de Ethernet (FCoE), controlador de máquina virtual (`virtio`), almacenamiento conectado en serie (SAS), unidades de memoria exprés no volátil (NVMe) y otros.

Un objetivo iSCSI puede ser un dispositivo físico dedicado en una red o un dispositivo lógico configurado por software iSCSI en un servidor de almacenamiento en red. El objetivo es el extremo del portal en una comunicación de bus de protocolo SCSI, para acceder al almacenamiento como números de unidad lógica (LUN).

El protocolo de canal de fibra a través de Ethernet (FCoE) transmite marcos de canal de fibra a través de redes Ethernet. Por lo general, los centros de datos tienen cableado dedicado de red de área de almacenamiento (SAN) y LAN, cada uno configurado de manera única para su tráfico. Con FCoE, ambos tipos de tráfico se pueden combinar en una arquitectura de red Ethernet convergente más grande. Los beneficios de FCoE incluyen menores costos de hardware y energía.

Multitrayecto

Una ruta es una conexión entre un servidor y el almacenamiento subyacente. Multitrayecto del asignador de dispositivos (`dm-multipath`) es una herramienta de múltiples rutas nativa de RHEL para configurar rutas de E/S redundantes en un único dispositivo lógico de agregación de rutas. Un dispositivo lógico creado con el asignador de dispositivos (`dm`) aparece como un dispositivo de bloque único en `/dev/mapper/` para cada LUN conectado al sistema.

La redundancia de múltiples rutas de almacenamiento también se puede implementar mediante la unión de redes cuando el almacenamiento, como iSCSI y FCoE, usa cableado de red.

Particiones

Un dispositivo de bloque se puede dividir en particiones. Las particiones pueden consumir todo el tamaño del dispositivo de bloque o dividir el dispositivo de bloque para crear varias particiones. Estas particiones se pueden usar para crear un sistema de archivos, dispositivos LVM o se pueden usar directamente para estructuras de bases de datos u otro almacenamiento sin formato.

RAID

Una matriz redundante de discos económicos (RAID) es una tecnología de virtualización de almacenamiento que crea grandes volúmenes lógicos a partir de varios componentes de dispositivos de bloques físicos o virtuales. Las diferentes formas de volúmenes RAID ofrecen redundancia de datos, mejora del rendimiento o ambas cosas, mediante la implementación de diseños de duplicación o división.

LVM soporta los niveles RAID 0, 1, 4, 5, 6 y 10. Los volúmenes lógicos RAID creados y administrados por LVM aprovechan los controladores del kernel de dispositivos múltiples (`mdadm`). Cuando no se usa LVM, Device Mapper RAID (`dm-raid`) proporciona una interfaz de asignación de dispositivos a los controladores del kernel `mdadm`.

Administrador de volúmenes lógicos

Los volúmenes físicos, los grupos de volúmenes y los volúmenes lógicos del LVM se analizaron en una sección anterior. LVM puede tomar casi cualquier forma de dispositivos de bloque físicos o virtuales, y crear almacenamiento como nuevos volúmenes de almacenamiento lógico, ocultando efectivamente la configuración de almacenamiento físico de las aplicaciones y otros clientes de almacenamiento.

Puede apilar volúmenes LVM e implementar funciones avanzadas, como cifrado y compresión, para cada parte de la pila (stack). Existen reglas obligatorias y prácticas recomendadas que se deben seguir para la creación de capas prácticas para escenarios específicos, pero esta introducción se centra solo en presentar los componentes. Las recomendaciones específicas para casos de uso se encuentran en la guía del usuario *Configuración y administración de volúmenes lógicos*.

LVM soporta el *cifrado LUKS*, donde un dispositivo de bloque inferior o una partición se cifra y se presenta como un volumen seguro para crear un sistema de archivos en la parte superior. La ventaja práctica de LUKS sobre el cifrado basado en sistemas de archivos o basado en archivos es que un dispositivo cifrado con LUKS no permite la visibilidad pública ni el acceso a la estructura del sistema de archivos, de modo que un dispositivo físico permanece seguro incluso cuando se elimina de una computadora.

LVM ahora incorpora la *desduplicación y compresión de VDO* como una función configurable de volúmenes lógicos regulares. El cifrado LUKS y VDO se pueden usar junto con volúmenes lógicos, con el cifrado LUKS de LVM habilitado en el volumen de VDO de LVM.

Sistema de archivos u otro uso

La capa superior de la pila (stack) suele ser un sistema de archivos, pero se puede usar como espacio sin formato para bases de datos o requisitos de datos de aplicaciones personalizados. RHEL soporta varios tipos de sistemas de archivos, pero recomienda XFS para la mayoría de los casos de uso modernos. Se requiere XFS cuando la utilidad que implementa LVM es Red Hat Ceph Storage o la herramienta de almacenamiento Stratis.

Las aplicaciones del servidor de bases de datos consumen almacenamiento de diferentes maneras, según su arquitectura y tamaño. Algunas bases de datos más pequeñas almacenan sus estructuras en archivos regulares que están contenidos en un sistema de archivos. Debido a la sobrecarga adicional o las restricciones de acceso al sistema de archivos, esta arquitectura tiene límites de escalamiento. Las bases de datos más grandes que desean omitir el almacenamiento en caché del sistema de archivos y usar sus propios mecanismos de almacenamiento en caché prefieren crear sus estructuras de base de datos en almacenamiento sin formato. Los volúmenes lógicos son adecuados para su uso en bases de datos y otros casos de uso de almacenamiento sin formato.

Red Hat Ceph Storage también prefiere crear sus propias estructuras de metadatos de administración de almacenamiento en dispositivos sin formato que se usarán para crear dispositivos de almacenamiento de objetos (OSD) de Ceph. En las últimas versiones de Red Hat Ceph Storage, Ceph usa LVM para inicializar dispositivos de disco para usar como OSD. Para obtener más información, consulte el curso *Cloud Storage with Red Hat Ceph Storage* (CL260).

Administración de almacenamiento de Stratis

Stratis es una herramienta de administración de almacenamiento local desarrollada por Red Hat y la comunidad upstream de Fedora. Stratis facilita la configuración inicial del almacenamiento, realizar cambios en la configuración del almacenamiento y usar funciones avanzadas de almacenamiento.



Importante

Stratis está disponible actualmente como Vista previa de tecnología, pero se espera que cuente con soporte en una versión posterior de RHEL 9. Para obtener información sobre el alcance de soporte de Red Hat para funciones de vista previa de tecnología, consulte el documento Alcance del soporte de las prestaciones de tecnología [<https://access.redhat.com/support/offering/techpreview>].

Red Hat recomienda a los clientes que envíen sus comentarios al implementar Stratis.

Stratis se ejecuta como un servicio que administra conjuntos (pools) de dispositivos de almacenamiento físico, y crea y administra de forma transparente los volúmenes para los sistemas de archivos recién creados.

Stratis compila los sistemas de archivos desde conjuntos (pools) de dispositivos de disco compartidos usando un concepto conocido como *aprovisionamiento ligero*. En lugar de asignar inmediatamente espacio físico de almacenamiento al sistema de archivos cuando lo crea, Stratis dinámicamente asigna ese espacio del conjunto (pool) a medida que el sistema de archivos almacena más datos. Por lo tanto, puede parecer que el sistema de archivos tiene un tamaño de 1 TiB, pero solo puede tener 100 GiB de almacenamiento real, que se le asignó realmente desde el conjunto (pool).

Puede crear múltiples conjuntos (pools) con diferentes dispositivos de almacenamiento. Desde cada conjunto (pool), puede crear uno o más sistemas de archivos. Actualmente, puede crear hasta 2^{24} sistemas de archivos por conjunto (pool).

Stratis compila los componentes que conforman un sistema de archivos administrado por Stratis a partir de componentes estándares de Linux. Internamente, Stratis usa la infraestructura del asignador de dispositivos que también usa LVM. Stratis formatea los sistemas de archivos administrados con XFS.

Figura 10.3 ilustra cómo Stratis ensambla los elementos de la solución de administración de almacenamiento. Stratis asigna dispositivos de almacenamiento de bloques, como discos duros o SSD, a conjuntos (pools), cada uno de los cuales contribuye a un almacenamiento físico en el conjunto. A continuación, crea sistemas de archivos a partir de los conjuntos (pools) y asigna el almacenamiento físico a cada sistema de archivos según sea necesario.

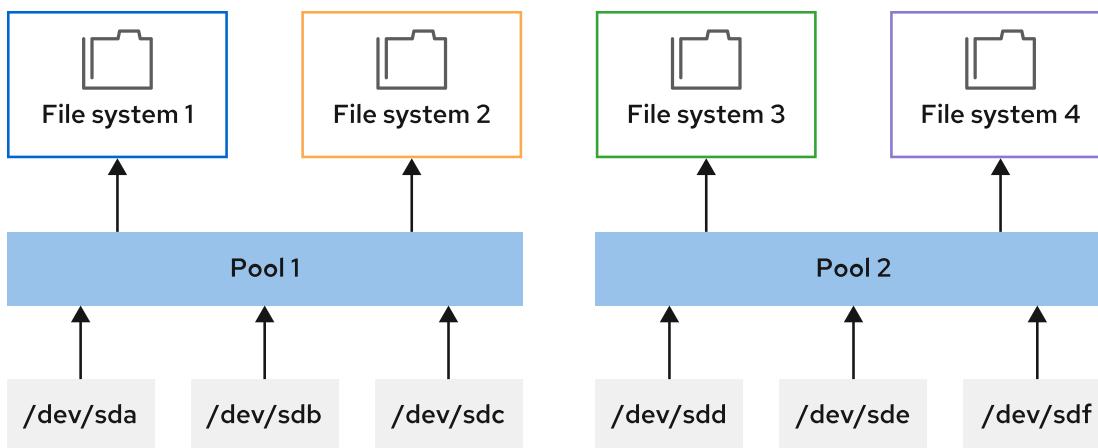


Figura 10.3: Arquitectura de Stratis

Métodos de administración de Stratis

Para administrar los sistemas de archivos con la solución de administración de almacenamiento Stratis, instale los paquetes `stratis-cli` y `stratisd`. El paquete `stratis-cli` proporciona el comando `stratis`, que envía solicitudes de reconfiguración al daemon del sistema `stratisd`. El paquete `stratisd` proporciona el servicio `stratisd`, que maneja los pedidos de reconfiguración, y administra y monitorea los dispositivos de bloque, los conjuntos (pools) y los sistemas de archivos de Stratis.

La administración de Stratis está incluida en la consola web de RHEL.

**Advertencia**

Reconfigure los sistemas de archivos creados por Stratis solo con herramientas y comandos de Stratis.

Stratis usa metadatos almacenados para reconocer conjuntos (pools) administrados, volúmenes y sistemas de archivos. La configuración manual de los sistemas de archivos Stratis con comandos que no son de Stratis podría causar la sobrescritura de esos metadatos e impedir que Stratis reconozca los sistemas de archivos que ha creado.

Instalación y habilitación de Stratis

Para usar Stratis, asegúrese de que su sistema tenga el software requerido y de que el servicio `stratisd` se esté ejecutando. Instale los paquetes `stratis-cli` y `stratisd`, inicie y habilite el servicio `stratisd`.

```
[root@host ~]# dnf install stratis-cli stratisd
...output omitted...
Is this ok [y/N]: y
...output omitted...
Complete!
[root@host ~]# systemctl enable --now stratisd
```

Creación de conjuntos (pools) de Stratis

Cree conjuntos (pools) de uno o más dispositivos de bloque con el comando `stratis pool create`. A continuación, use el comando `stratis pool list` para ver la lista de conjuntos (pools) disponibles.

```
[root@host ~]# stratis pool create pool1 /dev/vdb
[root@host ~]# stratis pool list
Name          Total Physical  Properties           UUID
pool1    5 GiB / 37.63 MiB / 4.96 GiB   ~Ca,-Cr   11f6f3c5-5...
```

**Advertencia**

El comando `stratis pool list` muestra el espacio de almacenamiento real que está en uso y el espacio del conjunto (pool) que aún está disponible. Actualmente, si un conjunto se llena, los datos adicionales escritos en los sistemas de archivos del conjunto (pool) se descartan discretamente.

Use el comando `stratis pool add-data` para agregar dispositivos de bloque adicionales a un conjunto (pool). A continuación, use el comando `stratis blockdev list` para verificar los dispositivos de bloque de un conjunto (pool).

```
[root@host ~]# stratis pool add-data pool1 /dev/vdc
[root@host ~]# stratis blockdev list pool1
Pool Name  Device Node  Physical Size  Tier
pool1      /dev/vdb        5 GiB     Data
pool1      /dev/vdc        5 GiB     Data
```

Administración de sistemas de archivos de Stratis

Use el comando `stratis filesystem create` para crear un sistema de archivos de un conjunto (pool). Los enlaces a los sistemas de archivos Stratis están en el directorio `/dev/stratis/pool1`. Use el comando `stratis filesystem list` para ver la lista de sistemas de archivos disponibles.

```
[root@host ~]# stratis filesystem create pool1 fs1
[root@host ~]# stratis filesystem list
Pool Name      Name    Used     Created          Device           UUID
pool1          fs1     546 MiB   Apr 08 2022 04:05  /dev/stratis/pool1/fs1
c7b57191...
```

Cree una instantánea del sistema de archivos Stratis con el comando `stratis filesystem snapshot`. Las capturas de instantáneas son independientes de los sistemas de archivos de origen. Stratis asigna dinámicamente el espacio de almacenamiento de instantáneas y usa 560 MB iniciales para almacenar el diario (journal) del sistema de archivos.

```
[root@host ~]# stratis filesystem snapshot pool1 fs1 snapshot1
```

Montaje de manera persistente de sistemas de archivos de Stratis

Para asegurarse de que los sistemas de archivos Stratis se monten de forma persistente, edite el archivo `/etc/fstab` y especifique los detalles del sistema de archivos. Use el comando `lsblk` para mostrar el UUID del sistema de archivos que debe usar en el archivo `/etc/fstab` para identificar el sistema de archivos. También puede usar el comando `stratis filesystem list` para obtener el UUID del sistema de archivos.

```
[root@host ~]# lsblk --output=UUID /dev/stratis/pool1/fs1
UUID
c7b57190-8fba-463e-8ec8-29c80703d45e
```

La siguiente es una entrada de ejemplo en el archivo `/etc/fstab` para montar de forma persistente un sistema de archivos Stratis. Esta entrada de ejemplo es una sola línea extensa en el archivo. La opción de montaje `x-systemd.requires=stratisd.service` retrasa el montaje del sistema de archivos hasta después de que el daemon `systemd` inicia el servicio `stratisd` durante el proceso de arranque.

```
UUID=c7b57190-8fba-463e-8ec8-29c80703d45e /dir1 xfs defaults,x-
systemd.requires=stratisd.service 0 0
```



Importante

Si no incluye la opción de montaje `x-systemd.requires=stratisd.service` en el archivo `/etc/fstab` para cada sistema de archivos Stratis, la máquina no se iniciará correctamente y se abortará en caso de `emergency.target` la próxima vez que la reinicie.



Advertencia

No use el comando `df` para consultar el espacio del sistema de archivos Stratis.

El comando `df` informa que cualquier sistema de archivos XFS administrado por Stratis tiene un tamaño de 1 TiB, independientemente de la asignación actual. Debido a que el sistema de archivos tiene un aprovisionamiento ligero, es posible que un conjunto (pool) no tenga suficiente almacenamiento físico para respaldar todo el sistema de archivos. Otros sistemas de archivos en el conjunto (pool) podrían usar todo el almacenamiento disponible.

Por lo tanto, es posible consumir todo el conjunto (pool) de almacenamiento, incluso cuando el comando `df` informa que el sistema de archivos tiene espacio disponible. Escribir en un sistema de archivos sin almacenamiento de conjunto (pool) disponible puede fallar.

En su lugar, use siempre el comando `stratis pool list` para monitorear con precisión el almacenamiento disponible de un conjunto (pool).



Referencias

Para obtener más información, consulte *Deduplicating And Compressing Logical Volumes On RHEL* en

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/deduplicating_and_compressing_logical_volumes_on_rhel/index

Para obtener más información, consulte *Red Hat Enterprise Linux 9 Managing File Systems Guide* en

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/managing_file_systems

Almacenamiento de Stratis

<https://stratis-storage.github.io/>

Lecciones que Stratis aprendió de ZFS, Btrfs y Linux Volume Manager

<https://opensource.com/article/18/4/stratis-lessons-learned>

► Ejercicio Guiado

Administración de almacenamiento en capas

En este ejercicio, usa Stratis para crear sistemas de archivos a partir de conjuntos (pools) de almacenamiento provistos por dispositivos de almacenamiento físicos.

Resultados

- Crear un sistema de archivos con aprovisionamiento ligero con la solución de administración de almacenamiento Stratis.
- Verificar que los volúmenes Stratis crezcan dinámicamente para soportar crecimiento de datos en tiempo real.
- Acceder a los datos desde la instantánea de un sistema de archivos con aprovisionamiento ligero.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start lvm-stratis
```

Instrucciones

- 1. Inicie sesión en la máquina `servera` como el usuario `student` y cambie al usuario `root`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

- 2. Instale los paquetes `stratisd` y `stratis-cli`.

```
[root@servera ~]# dnf install stratisd stratis-cli
...output omitted...
Is this ok [y/N]: y
...output omitted...
Complete!
```

- 3. Active el servicio `stratisd`.

```
[root@servera ~]# systemctl enable --now stratisd
```

- 4. Asegúrese de que el conjunto (pool) de Stratis **stratispool1** existe con el dispositivo de bloque `/dev/vdb`.

- 4.1. Cree el conjunto (pool) de Stratis **stratispool1**.

```
[root@servera ~]# stratis pool create stratispool1 /dev/vdb
```

- 4.2. Verifique la disponibilidad del conjunto (pool) **stratispool1**. Observe el tamaño del conjunto (pool).

Name	Total	Physical	Properties	UUID
stratispool1	5 GiB	/ 37.63 MiB / 4.96 GiB	~Ca,~Cr	3557c389-7...

- 5. Amplíe la capacidad del conjunto (pool) **stratispool1** con el dispositivo de bloque `/dev/vdc`.

- 5.1. Agregue el dispositivo de bloque `/dev/vdc` al conjunto (pool) **stratispool1**.

```
[root@servera ~]# stratis pool add-data stratispool1 /dev/vdc
```

- 5.2. Verifique el tamaño del conjunto (pool) **stratispool1**. El tamaño del conjunto (pool) **stratispool1** aumenta cuando agrega el dispositivo de bloque.

Name	Total	Physical	Properties	UUID
stratispool1	10 GiB	/ 41.63 MiB / 9.96 GiB	~Ca,~Cr	3557c389-7...

- 5.3. Verifique los dispositivos de bloque que son actualmente miembros del conjunto (pool) **stratispool1**.

```
[root@servera ~]# stratis blockdev list stratispool1
Pool Name      Device Node  Physical Size  Tier
stratispool1   /dev/vdb       5 GiB    Data
stratispool1   /dev/vdc       5 GiB    Data
```

- 6. Agregue un sistema de archivos con aprovisionamiento ligero denominado **stratis-filesystem1** en el conjunto (pool) **stratispool1**. Monte el sistema de archivos en el directorio `/stratisvol`. Cree un archivo en el sistema de archivos **stratis-filesystem1** denominado **file1** que contenga el texto **Hello World!**. Modifique el archivo `/etc/fstab` para montar de forma persistente el sistema de archivos en el directorio `/stratisvol`. Reinicie su sistema y verifique que el sistema de archivos se monte de manera persistente en los reinicios.

- 6.1. Cree el sistema de archivos con aprovisionamiento ligero **stratis-filesystem1** en el conjunto (pool) **stratispool1**. Puede tardar hasta un minuto para que se complete el comando.

```
[root@servera ~]# stratis filesystem create stratispool1 stratis-filesystem1
```

- 6.2. Verifique la disponibilidad del sistema de archivos **stratis-filesystem1**. Observe el uso actual del sistema de archivos **stratis-filesystem1**. Este uso del sistema de archivos aumentará a pedido en los siguientes pasos.

```
[root@servera ~]# stratis filesystem list
Pool Name      Name          Used      Created      Device
              UUID
stratispool1   stratis-filesystem1  546 MiB  Apr 08 2022 07:12  /dev/stratis/
stratispool1/stratis-filesystem1  48e8...
```

- 6.3. Cree el directorio **/stratisvol**.

```
[root@servera ~]# mkdir /stratisvol
```

- 6.4. Monte el sistema de archivos **stratis-filesystem1** en el directorio **/stratisvol**.

```
[root@servera ~]# mount /dev/stratis/stratispool1/stratis-filesystem1 \
/stratisvol
```

- 6.5. Verifique que el volumen **stratis-filesystem1** esté montado en el directorio **/stratisvol**.

```
[root@servera ~]# mount
...output omitted...
/dev/mapper/stratis-1-3557...fb3-thin-fs-48e8...9ebe on /stratisvol type xfs
(rw,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=32k,sunit=2048,swidth=2048,
noquota)
```

- 6.6. Cree el archivo de texto **/stratisvol/file1**.

```
[root@servera ~]# echo "Hello World!" > /stratisvol/file1
```

- 6.7. Obtenga el UUID del sistema de archivos. Tenga en cuenta que el UUID podría ser diferente en su sistema.

```
[root@servera ~]# lsblk --output=UUID \
/dev/stratis/stratispool1/stratis-filesystem1
UUID
d18cb4fc-753c-473a-9ead-d6661533b475
```

- 6.8. Modifique el archivo **/etc/fstab** para montar de forma persistente el sistema de archivos en el directorio **/stratisvol**. Para ello, use el comando **vim /etc/fstab** y agregue la siguiente línea. Reemplace el UUID por el correcto para su sistema.

```
UUID=d18c... /stratisvol xfs defaults,x-systemd.requires=stratisd.service 0 0
```

- 6.9. Reinicie su sistema y verifique que el sistema de archivos se monte de manera persistente en los reinicios.

```
[root@servera ~]# systemctl reboot
...output omitted...
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]# mount
...output omitted...
/dev/mapper/stratis-1-3557...fbd3-thin-fs-d18c...b475 on /stratisvol type xfs
(rw,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=32k,sunit=2048,swidth=2048,
noquota,x-systemd.requires=stratisd.service)
```

- 7. Verifique que el sistema de archivos con aprovisionamiento ligero **stratis-filesystem1** crece dinámicamente a medida que crecen los datos en el sistema de archivos.

7.1. Vea el uso actual del sistema de archivos **stratis-filesystem1**.

```
[root@servera ~]# stratis filesystem list
Pool Name      Name          Used       Created        Device
                  UUID
stratispool1   stratis-filesystem1  546 MiB  Apr 08 2022 07:12  /dev/stratis/
stratispool1/stratis-filesystem1    48e8...
```

7.2. Cree un archivo de 2 GiB en el sistema de archivos **stratis-filesystem1**. Puede tardar hasta un minuto para que se complete el comando.

```
[root@servera ~]# dd if=/dev/urandom of=/stratisvol/file2 bs=1M count=2048
```

7.3. Verifique el espacio usado en el sistema de archivos **stratis-filesystem1**.

La salida muestra que el espacio usado en el sistema de archivos **stratis-filesystem1** ha aumentado. El aumento del espacio usado confirma que el sistema de archivos de aprovisionamiento ligero se amplía dinámicamente según sea necesario.

```
[root@servera ~]# stratis filesystem list
Pool Name      Name          Used       Created        Device
                  UUID
stratispool1   stratis-filesystem1  2.60 GiB  Apr 08 2022 07:12  /dev/stratis/
stratispool1/stratis-filesystem1    48e8...
```

- 8. Cree una instantánea del sistema de archivos **stratis-filesystem1** denominada **stratis-filesystem1-snap**. La instantánea le proporcionará acceso a cualquier archivo que elimine del sistema de archivos **stratis-filesystem1**.

8.1. Cree una instantánea del sistema de archivos **stratis-filesystem1**. Puede tardar hasta un minuto para que se complete el comando.

```
[root@servera ~]# stratis filesystem snapshot stratispool1 \
stratis-filesystem1 stratis-filesystem1-snap
```

8.2. Verifique la disponibilidad de la instantánea.

```
[root@servera ~]# stratis filesystem list
Pool Name      Name          Used      Created      Device
                           UUID
stratispool1   stratis-filesystem1-snap  2.73 GiB  Apr 08 2022 07:22  /dev/
stratis/stratispool1/stratis-filesystem1-snap  5774...
stratispool1   stratis-filesystem1       2.73 GiB  Apr 08 2022 07:12  /dev/
stratis/stratispool1/stratis-filesystem1       48e8...
```

8.3. Quite el archivo /stratisvol/file1.

```
[root@servera ~]# rm /stratisvol/file1
rm: remove regular file '/stratisvol/file1'? y
```

8.4. Cree el directorio /stratisvol-snap.

```
[root@servera ~]# mkdir /stratisvol-snap
```

8.5. Monte la instantánea stratis-filesystem1-snap en el directorio /stratisvol-snap.

```
[root@servera ~]# mount /dev/stratis/stratispool1/stratis-filesystem1-snap \
/stratisvol-snap
```

8.6. Verifique que aún puede acceder al archivo que eliminó del sistema de archivos stratis-filesystem1 en la instantánea.

```
[root@servera ~]# cat /stratisvol-snap/file1
Hello World!
```

► 9. Desmonte los volúmenes /stratisvol y /stratisvol-snap.

```
[root@servera ~]# umount /stratisvol-snap
[root@servera ~]# umount /stratisvol
```

► 10. Elimine el sistema de archivos con aprovisionamiento ligero stratis-filesystem1 y su instantánea stratis-filesystem1-snap del sistema.

10.1. Destruya la instantánea stratis-filesystem1-snap.

```
[root@servera ~]# stratis filesystem destroy stratispool1 stratis-filesystem1-snap
```

10.2. Destruya el sistema de archivos stratis-filesystem1.

```
[root@servera ~]# stratis filesystem destroy stratispool1 stratis-filesystem1
```

10.3. Regrese al sistema workstation como el usuario student.

```
[root@servera ~]# exit  
logout  
[student@servera ~]$ exit  
logout  
Connection to servera closed.  
[student@workstation ~]$
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish lvm-stratis
```

Esto concluye la sección.

► Trabajo de laboratorio

Administración de la pila (stack) de almacenamiento

En este trabajo de laboratorio, modifica el tamaño de un volumen lógico existente, agrega recursos de LVM según sea necesario y, luego, agrega un nuevo volumen lógico con un sistema de archivos XFS montado de manera persistente en este.

Resultados

- Cambiar el tamaño del volumen lógico `serverb_01_lv` a 768 MiB.
- Cree el nuevo volumen lógico `serverb_02_lv` con 128 MiB con un sistema de archivos XFS.
- Monte el volumen de manera persistente en el directorio `/storage/data2`.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start lvm-review
```

Instrucciones

En la máquina `serverb`, el volumen lógico `serverb_01_lv` montado en el directorio `/storage/data1` se está quedando sin espacio en disco y debe ampliarse a 768 MiB. Debe asegurarse de que el LV `serverb_01_lv` permanece montado de forma persistente en el directorio `/storage/data1`.

El LV `serverb_01_lv` está presente en el grupo de volúmenes `serverb_01_vg`.

Desafortunadamente, no tiene espacio suficiente para ampliar el volumen lógico existente. Existe una partición de 512 MiB en el disco `/dev/vdb`. Cree una nueva partición con el tamaño sucesivo de 512 MiB en el disco `/dev/vdb`.

Cree el LV `serverb_02_lv` con 128 MiB. Cree el sistema de archivos XFS en el volumen creado recientemente. Monte el volumen lógico recién creado en el directorio `/storage/data2`

1. Cree una partición de 512 MiB en el disco `/dev/vdb`. Inicialice esta partición como volumen físico y amplíe el grupo de volúmenes `serverb_01_vg` para usar esta partición.
2. Amplíe el volumen lógico `serverb_01_lv` a 768 MiB.
3. En el grupo de volúmenes existente, cree un nuevo volumen lógico `serverb_02_lv` con 128 MiB. Agregue un sistema de archivos XFS y móntelo de forma persistente en el directorio `/storage/data2`.
4. Verifique que el LV creado recientemente esté montado con el tamaño deseado.

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `Lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade lvm-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `Lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish lvm-review
```

Esto concluye la sección.

► Solución

Administración de la pila (stack) de almacenamiento

En este trabajo de laboratorio, modifica el tamaño de un volumen lógico existente, agrega recursos de LVM según sea necesario y, luego, agrega un nuevo volumen lógico con un sistema de archivos XFS montado de manera persistente en este.

Resultados

- Cambiar el tamaño del volumen lógico `serverb_01_lv` a 768 MiB.
- Cree el nuevo volumen lógico `serverb_02_lv` con 128 MiB con un sistema de archivos XFS.
- Monte el volumen de manera persistente en el directorio `/storage/data2`.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start lvm-review
```

Instrucciones

En la máquina `serverb`, el volumen lógico `serverb_01_lv` montado en el directorio `/storage/data1` se está quedando sin espacio en disco y debe ampliarse a 768 MiB. Debe asegurarse de que el LV `serverb_01_lv` permanece montado de forma persistente en el directorio `/storage/data1`.

El LV `serverb_01_lv` está presente en el grupo de volúmenes `serverb_01_vg`. Desafortunadamente, no tiene espacio suficiente para ampliar el volumen lógico existente. Existe una partición de 512 MiB en el disco `/dev/vdb`. Cree una nueva partición con el tamaño sucesivo de 512 MiB en el disco `/dev/vdb`.

Cree el LV `serverb_02_lv` con 128 MiB. Cree el sistema de archivos XFS en el volumen creado recientemente. Monte el volumen lógico recién creado en el directorio `/storage/data2`

1. Cree una partición de 512 MiB en el disco `/dev/vdb`. Inicialice esta partición como volumen físico y amplíe el grupo de volúmenes `serverb_01_vg` para usar esta partición.
 - 1.1. Inicie sesión en la máquina `serverb` como el usuario `student` y cambie al usuario `root`.

```
[student@workstation ~]$ ssh student@serverb  
...output omitted...  
[student@serverb ~]$ sudo -i  
[sudo] password for student: student  
[root@serverb ~]#
```

- 1.2. Cree la partición de 512 MiB y establezca el tipo de partición lvm.

```
[root@serverb ~]# parted /dev/vdb mkpart primary 514MiB 1026MiB  
[root@serverb ~]# parted /dev/vdb set 2 lvm on
```

- 1.3. Registre la nueva partición con el kernel.

```
[root@serverb ~]# udevadm settle
```

- 1.4. Inicialice la partición como un PV.

```
[root@serverb ~]# pvcreate /dev/vdb2  
Physical volume "/dev/vdb2" successfully created.
```

- 1.5. Exienda el VG `serverb_01_vg` con el nuevo PV `/dev/vdb2`.

```
[root@serverb ~]# vgextend serverb_01_vg /dev/vdb2  
Volume group "serverb_01_vg" successfully extended
```

2. Amplíe el volumen lógico `serverb_01_lv` a 768 MiB.

- 2.1. Amplíe el LV `serverb_01_lv` a 768 MiB.

O también podría usar la opción `-L +512M` del comando `lvcreate` para cambiar el tamaño del LV.

```
[root@serverb ~]# lvextend -L 768M /dev/serverb_01_vg/serverb_01_lv  
Size of logical volume serverb_01_vg/serverb_01_lv changed from 256.00 MiB (64  
extents) to 768.00 MiB (192 extents).  
Logical volume serverb_01_vg/serverb_01_lv successfully resized.
```

- 2.2. Amplíe el sistema de archivos XFS que consume el espacio restante del LV.

```
[root@serverb ~]# xfs_growfs /storage/data1  
meta-data=/dev/mapper/serverb_01_vg-serverb_01_lv isize=512    agcount=4,  
agsize=16384 blks  
...output omitted...  
data blocks changed from 65536 to 196608
```



nota

El comando `xfs_growfs` introduce un paso adicional para ampliar el sistema de archivos. Una alternativa sería usar la opción `-r` del comando `lvextend`.

3. En el grupo de volúmenes existente, cree un nuevo volumen lógico **serverb_02_lv** con 128 MiB. Agregue un sistema de archivos XFS y móntelo de forma persistente en el directorio **/storage/data2**.

- 3.1. Cree el LV **serverb_02_lv** con 128 MiB desde el VG **serverb_01_vg**.

```
[root@serverb ~]# lvcreate -n serverb_02_lv -L 128M serverb_01_vg
Logical volume "serverb_02_lv" created.
```

- 3.2. Cree el sistema de archivos xfs en el LV **serverb_02_lv**.

```
[root@serverb ~]# mkfs -t xfs /dev/serverb_01_vg/serverb_02_lv
...output omitted...
```

- 3.3. Cree el directorio **/storage/data2** como el punto de montaje.

```
[root@serverb ~]# mkdir /storage/data2
```

- 3.4. Agregue la línea siguiente al final del archivo **/etc/fstab**:

```
/dev/serverb_01_vg/serverb_02_lv /storage/data2 xfs defaults 0 0
```

- 3.5. Actualice el daemon **systemd** con el nuevo archivo de configuración **/etc/fstab**.

```
[root@serverb ~]# systemctl daemon-reload
```

- 3.6. Monte el LV **serverb_02_lv**.

```
[root@serverb ~]# mount /storage/data2
```

4. Verifique que el LV creado recientemente esté montado con el tamaño deseado.

- 4.1. Use el comando **df** para verificar el tamaño del LV **serverb_01_lv**.

```
[root@serverb ~]# df -h /storage/data1
Filesystem           Size   Used  Avail Use% Mounted on
/dev/mapper/serverb_01_vg-serverb_01_lv  763M   19M  744M   3% /storage/data1
```

- 4.2. Verifique el tamaño del LV **serverb_02_lv**.

```
[root@serverb ~]# df -h /storage/data2
Filesystem           Size   Used  Avail Use% Mounted on
/dev/mapper/serverb_01_vg-serverb_02_lv  123M   7.6M  116M   7% /storage/data2
```

- 4.3. Verifique los detalles del LV **serverb_01_lv**.

```
[root@serverb ~]# lvdisplay /dev/serverb_01_vg/serverb_01_lv
--- Logical volume ---
  LV Path         /dev/serverb_01_vg/serverb_01_lv
  LV Name        serverb_01_lv
```

```

VG Name          serverb_01_vg
LV UUID          1pY3DZ-fs1F-mptC-fL32-e8tG-PFBT-bs7LSJ
LV Write Access  read/write
LV Creation host, time serverb.lab.example.com, 2022-05-05 14:40:51 -0400
LV Status        available
# open           1
LV Size          768.00 MiB
Current LE       192
Segments         2
Allocation       inherit
Read ahead sectors auto
- currently set to 8192
Block device    253:0

```

4.4. Verifique los detalles del LV `serverb_02_lv`.

```

[root@serverb ~]# lvdisplay /dev/serverb_01_vg/serverb_02_lv
--- Logical volume ---
LV Path          /dev/serverb_01_vg/serverb_02_lv
LV Name          serverb_02_lv
VG Name          serverb_01_vg
LV UUID          0aJIB6-Ti2b-jLCk-imB6-rkLx-mUoX-acjkz9
LV Write Access  read/write
LV Creation host, time serverb.lab.example.com, 2022-05-05 14:45:46 -0400
LV Status        available
# open           1
LV Size          128.00 MiB
Current LE       32
Segments         1
Allocation       inherit
Read ahead sectors auto
- currently set to 8192
Block device    253:1

```

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade lvm-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish lvm-review
```

Esto concluye la sección.

Resumen

- Puede usar LVM para crear un almacenamiento flexible al asignar espacio en múltiples dispositivos de almacenamiento.
- Puede administrar los volúmenes físicos, los grupos de volúmenes y los volúmenes lógicos mediante los comandos `pvcreate`, `vgreduce` y `lvextend`.
- Puede formatear los volúmenes lógicos con un sistema de archivos o espacio de intercambio (`swap`), y montarlos de forma persistente.
- Puede agregar almacenamiento a los grupos de volúmenes y los volúmenes lógicos pueden ampliarse de forma dinámica.
- Puede usar las capas y los componentes de la pila (stack) de almacenamiento para administrar el almacenamiento de manera eficiente.
- Puede usar el optimizador de datos virtual (VDO) para la compresión y desduplicación de datos en el almacenamiento LVM.
- Puede usar Stratis para realizar una configuración de almacenamiento inicial o habilitar funciones de almacenamiento avanzadas.

capítulo 11

Servicios de control y proceso de arranque

Meta

Controlar y monitorear los servicios de red, los daemons del sistema y el proceso de arranque con 'systemd'.

Objetivos

- Enumerar los daemons del sistema y los servicios de red iniciados por el servicio systemd y las unidades socket.
- Controlar los daemons del sistema y los servicios de red con systemctl.
- Describir el proceso de arranque de Red Hat Enterprise Linux, configurar el objetivo predeterminado que se usa en el arranque e iniciar un sistema con un objetivo no predeterminado.
- Iniciar sesión en un sistema y cambiar la contraseña de root cuando la actual se haya perdido.
- Reparar manualmente la configuración del sistema de archivos o problemas de daños que detengan el proceso de arranque.

Secciones

- Identificación de procesos del sistema iniciados en forma automática (y ejercicio guiado)
- Control de servicios del sistema (y ejercicio guiado)
- Selección del objetivo de arranque (y ejercicio guiado)
- Restablecimiento de la contraseña de root (y ejercicio guiado)
- Reparación de problemas de sistemas de archivos en el arranque (y ejercicio guiado)

Trabajo de laboratorio

- Control del proceso de arranque

Identificación de procesos del sistema iniciados en forma automática

Objetivos

Enumerar daemons del sistema y los servicios de red iniciados por el servicio `systemd` y las unidades socket.

Introducción al daemon del sistema

El daemon `systemd` administra el proceso de inicio para Linux, incluido el inicio del servicio y la gestión de servicios en general. El daemon `systemd` activa los recursos del sistema, los daemons del servidor y otros procesos, tanto en el momento del arranque como en un sistema que está en funcionamiento.

Los daemons son procesos que esperan o se ejecutan en segundo plano y realizan diversas tareas. Generalmente, los daemons se inician automáticamente en el momento del arranque y continúan ejecutándose hasta que se apaga el sistema o usted los detiene manualmente. Por convención, los nombres de los daemons finalizan con la letra d.

Un servicio en el sentido `systemd` a menudo se refiere a uno o más daemons. Sin embargo, iniciar o detener un servicio puede cambiar el estado del sistema una vez, sin dejar un proceso daemon en ejecución después (denominado oneshot).

En Red Hat Enterprise Linux, el primer proceso que se inicia (PID1) es el daemon `systemd`, que aporta estas funciones:

- Capacidades de paralelización (inicio de múltiples servicios de forma simultánea), que aumentan la velocidad de arranque de un sistema.
- Inicio a pedido de los daemons sin necesidad de otro servicio.
- Gestión automática de dependencias del servicio, que puede evitar largos tiempos de espera. Por ejemplo, un servicio que depende de una red no intenta iniciarse hasta que la red esté disponible.
- Método para realizar el seguimiento de los procesos relacionados en forma conjunta con el uso de los grupos de control de Linux.

Descripción de las unidades de servicio

El daemon `systemd` usa *unidades* para administrar diferentes tipos de objetos:

- Las *unidades de servicio* tienen una extensión `.service` y representan servicios del sistema. Puede usar estas unidades de servicio para iniciar los daemons usados con más frecuencia, como un servidor web.
- Las *unidades de socket* tienen una extensión `.socket` y representan sockets de comunicación entre procesos (IPC) que `systemd` debe monitorear. Si un cliente se conecta al socket, el gerente `systemd` iniciará un daemon y le pasará la conexión. Puede usar unidades socket para demorar el inicio de un servicio en el momento del arranque y para iniciar servicios usados con menos frecuencia a pedido.
- Las *unidades de ruta* tienen una extensión `.path` y se usan para demorar la activación de un servicio hasta que ocurra un cambio en el sistema de archivos específico. Puede usar unidades de ruta para servicios que usan directorios de cola, como un sistema de impresión.

Para administrar unidades, use el comando `systemctl`. Por ejemplo, el comando `systemctl -t help` permite visualizar los tipos de unidad disponibles. El comando `systemctl` puede abreviar los nombres de las unidades, las entradas de árbol de proceso y las descripciones de unidad.

Enumeración de unidades de servicio

Use el comando `systemctl` para analizar el estado actual del sistema. Por ejemplo, el siguiente comando enumera y ordena las páginas de todas las unidades de servicio cargadas actualmente.

```
[root@host ~]# systemctl list-units --type=service
UNIT           LOAD   ACTIVE   SUB      DESCRIPTION
atd.service    loaded  active   running  Job spooling tools
auditd.service loaded  active   running  Security Auditing Service
chronyd.service loaded  active   running  NTP client/server
crond.service  loaded  active   running  Command Scheduler
dbus.service   loaded  active   running  D-Bus System Message Bus
...output omitted...
```

En este ejemplo, la opción `--type=service` limita el tipo de unidades `systemd` a unidades de servicio. La salida tiene las siguientes columnas:

UNIT

El nombre de la unidad de servicio.

LOAD

Se detalla si el daemon `systemd` analizó adecuadamente la configuración de la unidad y cargó la unidad en la memoria.

ACTIVE

El estado de activación de alto nivel de la unidad. Esta información indica si la unidad se inició de forma satisfactoria.

SUB

El estado de activación de bajo nivel de la unidad. Esta información proporciona datos más detallados sobre la unidad. La información varía según el tipo de unidad, el estado y cómo se ejecuta la unidad.

DESCRIPTION

La descripción breve de la unidad.

De manera predeterminada, el comando `systemctl list-units --type=service` enumera solamente las unidades de servicio con estados de activación `active` (activos). La opción `systemctl list-units --all` enumera todas las unidades de servicio, independientemente de los estados de activación. Use la opción `--state=` para filtrar los valores en los campos LOAD, ACTIVE o SUB.

```
[root@host ~]# systemctl list-units --type=service --all
UNIT           LOAD   ACTIVE   SUB      DESCRIPTION
atd.service    loaded  active   running  Job spooling tools
auditd.service loaded  active   running  Security Auditing ...
auth-rpcgss-module.service loaded  inactive dead    Kernel Module ...
chronyd.service loaded  active   running  NTP client/server
cpupower.service loaded  inactive dead    Configure CPU power ...
crond.service  loaded  active   running  Command Scheduler
```

```
dbus.service          loaded active running D-Bus System Message Bus
● display-manager.service    not-found inactive dead     display-manager.service
...output omitted...
```

El comando `systemctl` sin ningún argumento enumera las unidades que están cargadas y activas.

```
[root@host ~]# systemctl
UNIT                      LOAD ACTIVE SUB DESCRIPTION
proc-sys-fs-binfmt_misc.automount    loaded active waiting Arbitrary...
sys-devices-....device           loaded active plugged   Virtio network...
sys-subsystem-net-devices-ens3.device loaded active plugged   Virtio network...
...output omitted...
..mount                     loaded active mounted  Root Mount
boot.mount                 loaded active mounted  /boot
...output omitted...
systemd-ask-password-plymouth.path  loaded active waiting  Forward Password...
systemd-ask-password-wall.path     loaded active waiting  Forward Password...
init.scope                  loaded active running   System and Servi...
session-1.scope             loaded active running   Session 1 of...
atd.service                 loaded active running   Job spooling tools
audittd.service            loaded active running   Security Auditing...
chronyd.service            loaded active running   NTP client/server
crond.service              loaded active running   Command Scheduler
...output omitted...
```

El comando `systemctl` con la opción `list-units` muestra las unidades que el servicio `systemd` intenta analizar y cargar en la memoria. Esta opción no muestra los servicios que están instalados pero no habilitados. Puede usar el comando `systemctl` con la opción `list-unit-files` para ver el estado de todos los archivos de unidad instalados:

```
[root@host ~]# systemctl list-unit-files --type=service
UNIT FILE                      STATE      VENDOR PRESET
arp-ethers.service            disabled  disabled
atd.service                   enabled   enabled
audittd.service              enabled   enabled
auth-rpcgss-module.service   static    -
autovt@.service              alias    -
blk-availability.service     disabled  disabled
...output omitted...
```

En la salida del comando `systemctl list-unit-files`, algunas entradas comunes para el campo `STATE` son `enabled`, `disabled`, `static` y `masked`. Todos los valores `STATE` se enumeran en las páginas del manual de comandos `systemctl`.

Visualización de los estados de servicio

Vea el estado de una unidad con el comando `systemctl status name.type`. Si se omite el tipo de unidad, el comando espera una unidad de servicio con ese nombre.

```
[root@host ~]# systemctl status sshd.service
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2022-03-14 05:38:12 EDT; 25min ago
       Docs: man:sshd(8)
              man:sshd_config(5)
     Main PID: 1114 (sshd)
        Tasks: 1 (limit: 35578)
      Memory: 5.2M
         CPU: 64ms
      CGroup: /system.slice/sshd.service
              └─1114 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Mar 14 05:38:12 workstation systemd[1]: Starting OpenSSH server daemon...
Mar 14 05:38:12 workstation sshd[1114]: Server listening on 0.0.0.0 port 22.
Mar 14 05:38:12 workstation sshd[1114]: Server listening on :: port 22.
Mar 14 05:38:12 workstation systemd[1]: Started OpenSSH server daemon.
...output omitted...
```

Algunos campos de la salida del comando `systemctl` con la opción `status`:

Información de la unidad de servicio

Campo	Descripción
Loaded (Cargada)	Si la unidad de servicio está cargada en la memoria.
Active (Activa)	Si la unidad de servicio se está ejecutando y, de ser así, por cuánto tiempo lo ha hecho.
Docs (Documentos)	Dónde encontrar más información sobre el servicio.
Main PID (ID de proceso principal)	El ID de proceso principal del servicio, incluido el nombre del comando.
Status (Estado)	Más información sobre el servicio.
Process (Proceso)	Más información sobre los procesos relacionados.
CGroup (Grupo de control)	Más información sobre los grupos de control relacionados.

No todos estos campos están siempre presentes en la salida del comando.

Las palabras clave en la salida del estado indican el estado del servicio:

Estados de servicio en la salida de systemctl

Palabra clave	Descripción
loaded (cargado)	Se procesa el archivo de configuración de la unidad.
active (running) (activo [en ejecución])	El servicio se está ejecutando con procesos continuos.
active (exited) (activo [cerrado])	El servicio completó correctamente la configuración de una sola vez.
active (waiting) (activo [en espera])	El servicio está en ejecución, pero a la espera de un evento.
inactive (inactivo)	El servicio no se está ejecutando.
enabled (habilitado)	El servicio se inicia en el momento del arranque.
disabled (deshabilitado)	El servicio no está configurado para iniciarse en el momento del arranque.
static (estático)	El servicio 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` que se usaba en Red Hat Enterprise Linux 6 y versiones anteriores.

Verificación del estado de un servicio

El comando `systemctl` verifica los estados específicos de un servicio. Por ejemplo, use el comando `systemctl` con la opción `is-active` para verificar que la unidad de servicio se encuentre activa (en ejecución):

```
[root@host ~]# systemctl is-active sshd.service
active
```

El comando devuelve el estado de la unidad de servicio, el cual generalmente es `active` o `inactive`.

Ejecute el comando `systemctl` con la opción `is-enabled` para verificar si una unidad de servicio está habilitada para iniciarse automáticamente durante el arranque del sistema:

```
[root@host ~]# systemctl is-enabled sshd.service
enabled
```

El comando informa si la unidad de servicio está habilitada para iniciarse en el momento del arranque, lo cual generalmente se informa como `enabled` o `disabled`.

Para verificar si la unidad falló durante el arranque, ejecute el comando `systemctl` con la opción `is-failed`:

```
[root@host ~]# systemctl is-failed sshd.service  
active
```

El comando informa `active` si el servicio está ejecutándose correctamente o `failed` si se ha producido un error durante el arranque. Si la unidad se detuvo, devuelve `unknown` o `inactive`.

Para enumerar todas las unidades que han presentado un error, ejecute el comando `systemctl --failed --type=service`.



Referencias

Páginas del manual `systemd(1)`, `systemd.unit(5)`, `systemd.service(5)`, `systemd.socket(5)` y `systemctl(1)`

Para obtener más información, consulte el capítulo *Managing Services with systemd* de la *Red Hat Enterprise Linux 9 Configuring Basic System Settings Guide* en https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/configuring_basic_system_settings/managing-services-with-systemd_configuring-basic-system-settings#managing-services-with-systemd_configuring-basic-system-settings

► Ejercicio Guiado

Identificación de procesos del sistema iniciados en forma automática

En este ejercicio, enumerará las unidades de servicio instaladas e identificará qué servicios están actualmente habilitados y activos en un servidor.

Resultados

- Enumerar todas las unidades de servicio instaladas.
- Identificar los servicios activos y habilitados en el sistema.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start services-identify
```

Instrucciones

- 1. Use el comando `ssh` para iniciar sesión en la máquina `servera` con el usuario `student`.

```
[student@workstation ~]$ ssh student@servera
[student@servera ~]$
```

- 2. Enumere todas las unidades de servicio instaladas en la máquina `servera`.

```
[student@servera ~]$ systemctl list-units --type=service
UNIT                  LOAD     ACTIVE   SUB      DESCRIPTION
atd.service           loaded   active  running  Deferred execution scheduler
auditd.service        loaded   active  running  Security Auditing Service
chronyd.service       loaded   active  running  NTP client/server
crond.service         loaded   active  running  Command Scheduler
dbus-broker.service   loaded   active  running  D-Bus System Message Bus
...output omitted...
```

Presione `q` para salir del comando.

- 3. Enumere todas las unidades socket, activas e inactivas, en la máquina `servera`.

```
[student@servera ~]$ systemctl list-units --type=socket --all
UNIT                  LOAD     ACTIVE   SUB      DESCRIPTION
dbus.socket           loaded   active  running  D-Bus System Message Bus Socket
dm-event.socket       loaded   active  listening Device-mapper event daemon FIFOs
```

```
lvm2-lvmpolld.socket loaded active listening LVM2 poll daemon socket
...output omitted...

LOAD = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB = The low-level unit activation state, values depend on unit type.
13 loaded units listed.
To show all installed unit files use 'systemctl list-unit-files'.
```

- 4. Explore el estado del servicio `chrony`. Puede usar este servicio para la sincronización del protocolo de tiempo en red (NTP).

- 4.1. Muestre el estado del servicio `chrony`. Observe la ID del proceso de todos los daemons activos.

```
[student@servera ~]$ systemctl status chronyd
● chronyd.service - NTP client/server
   Loaded: loaded (/usr/lib/systemd/system/chronyd.service; enabled; vendor
   preset: enabled)
     Active: active (running) since Mon 2022-03-14 05:38:15 EDT; 1h 16min ago
       Docs: man:chrony(8)
              man:chrony.conf(5)
   Process: 728 ExecStart=/usr/sbin/chronyd $OPTIONS (code=exited, status=0/
 SUCCESS)
   Main PID: 747 (chronyd)
      Tasks: 1 (limit: 10800)
     Memory: 3.7M
        CPU: 37ms
      CGroup: /system.slice/chronyd.service
              └─747 /usr/sbin/chronyd -F 2

Mar 14 05:38:15 servera.lab.example.com systemd[1]: Starting NTP client/server...
Mar 14 05:38:15 servera.lab.example.com chronyd[747]: chronyd version 4.1 starting
(+CMDMON +NTP +REFCLOCK +RTC +PRIVDROP +SCFILTER +SIGND +ASYNCDNS +NTS +SECHASH
+IPV6 +DEBUG)
Mar 14 05:38:15 servera.lab.example.com chronyd[747]: commandkey directive is no
longer supported
Mar 14 05:38:15 servera.lab.example.com chronyd[747]: generatecommandkey directive
is no longer supported
Mar 14 05:38:15 servera.lab.example.com chronyd[747]: Frequency -11.870 +/- 1.025
ppm read from /var/lib/chrony/drift
Mar 14 05:38:15 servera.lab.example.com chronyd[747]: Loaded seccomp filter (level
2)
Mar 14 05:38:15 servera.lab.example.com systemd[1]: Started NTP client/server.
Mar 14 05:38:23 servera.lab.example.com chronyd[747]: Selected source
172.25.254.254
```

Presione q para salir del comando.

- 4.2. Confirme que el daemon `chrony` se está ejecutando usando su ID de proceso. En el comando anterior, la salida de la ID del proceso asociada con el servicio `chrony` es 747. La ID del proceso puede diferir en su sistema.

```
[student@servera ~]$ ps -p 747
 PID TTY      TIME CMD
 747 ?        00:00:00 chronyd
```

- 5. Explore el estado del servicio sshd. Puede usar este servicio para una comunicación cifrada segura entre sistemas.

- 5.1. Determine si el servicio sshd está habilitado para que se inicie en el arranque del sistema.

```
[student@servera ~]$ systemctl is-enabled sshd
enabled
```

- 5.2. Determine si el servicio sshd está activo sin mostrar toda la información de estado.

```
[student@servera ~]$ systemctl is-active sshd
active
```

- 5.3. Muestre el estado del servicio sshd.

```
[student@servera ~]$ systemctl status sshd
● sshd.service - OpenSSH server daemon
  Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
  Active: active (running) since Mon 2022-03-14 05:38:16 EDT; 1h 19min ago
    Docs: man:sshd(8)
          man:sshd_config(5)
 Main PID: 784 (sshd)
   Tasks: 1 (limit: 10800)
     Memory: 6.7M
       CPU: 82ms
      CGroup: /system.slice/sshd.service
              └─784 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Mar 14 05:38:16 servera.lab.example.com systemd[1]: Starting OpenSSH server
daemons...
Mar 14 05:38:16 servera.lab.example.com sshd[784]: Server listening on 0.0.0.0
port 22.
Mar 14 05:38:16 servera.lab.example.com sshd[784]: Server listening on :: port 22.
Mar 14 05:38:16 servera.lab.example.com systemd[1]: Started OpenSSH server daemon.
Mar 14 06:51:36 servera.lab.example.com sshd[1090]: Accepted publickey for student
from 172.25.250.9 port 53816 ssh2: RSA SHA256:M8ikhcEDm2tQ95Z0o7ZvufqEixCFCT
+wowZLNzNlBT0
Mar 14 06:51:36 servera.lab.example.com sshd[1090]: pam_unix(sshd:session):
  session opened for user student(uid=1000) by (uid=0)
```

Presione q para salir del comando.

- 6. Enumere los estados habilitados y deshabilitados de todas las unidades de servicio.

```
[student@servera ~]$ systemctl list-unit-files --type=service
UNIT FILE                      STATE      VENDOR PRESET
arp-ethers.service              disabled   disabled
atd.service                     enabled    enabled
auditd.service                 enabled    enabled
auth-rpcgss-module.service     static     -
autovt@.service                alias     -
blk-availability.service       disabled   disabled
bluetooth.service              enabled    enabled
chrony-wait.service            disabled   disabled
chronyd.service                enabled    enabled
...output omitted...
```

Presione q para salir del comando.

- 7. Regrese al sistema **workstation** como el usuario **student**.

```
[student@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation]$
```

Finalizar

En la máquina **workstation**, cambie al directorio de inicio de usuario **student** y use el comando **lab** para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish services-identify
```

Esto concluye la sección.

Control de servicios del sistema

Objetivos

Controlar los daemons del sistema y los servicios de red con `systemctl`.

Iniciar y detener servicios

Puede iniciar, detener o recargar servicios manualmente para actualizar el servicio, actualizar el archivo de configuración, desinstalar el servicio o administrar manualmente un servicio que se usa con poca frecuencia.

Use el comando `systemctl status` para verificar el estado del servicio y saber si el servicio está ejecutándose o está detenido.

```
[root@host ~]# systemctl status sshd.service
● sshd.service - OpenSSH server daemon
  Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
  Active: active (running) since Wed 2022-03-23 11:58:18 EDT; 2min 56s ago
    ...output omitted...
```

A continuación, use el comando `systemctl start` como el usuario `root` (con el comando `sudo` si es necesario). Si ejecuta el comando `systemctl start` con el nombre del servicio solamente (sin el tipo de servicio), el servicio `systemd` busca archivos `.service`.

```
[root@host ~]# systemctl start sshd
```

Para detener un servicio en ejecución, use el comando `systemctl` con la opción `stop`. En los siguientes ejemplos, se muestra cómo detener el servicio `sshd.service`:

```
[root@host ~]# systemctl stop sshd.service
```

Reiniciar y recargar servicios

Cuando reinicia un servicio en ejecución, el servicio primero se detiene y, luego, se inicia nuevamente. Al reiniciar el servicio, el nuevo proceso obtiene una nueva ID durante el arranque y, por lo tanto, se modifica la ID del proceso. Para reiniciar un servicio en ejecución, use el comando `systemctl` con la opción `restart`. En los siguientes ejemplos, se muestra cómo reiniciar el servicio `sshd`:

```
[root@host ~]# systemctl restart sshd.service
```

Algunos servicios pueden recargar sus archivos de configuración sin requerir un reinicio, lo que se denomina *recarga de servicio*. La recarga de un servicio no cambia la ID del proceso asociada con diversos procesos del servicio. Para volver a cargar un servicio en ejecución, use el comando `systemctl` con la opción `reload`. En el siguiente ejemplo, se muestra cómo volver a cargar el servicio `sshd.service` después de modificar la configuración:

```
[root@host ~]# systemctl reload sshd.service
```

En caso de que no esté seguro de si el servicio cuenta con la funcionalidad para volver a cargar los cambios del archivo de configuración, use el comando `systemctl` con la opción `reload-or-restart`. El comando vuelve a cargar los cambios de configuración si la función de recarga está disponible. De lo contrario, el comando reinicia el servicio para implementar los nuevos cambios de configuración:

```
[root@host ~]# systemctl reload-or-restart sshd.service
```

Enumeración de dependencias de la unidad

Algunos servicios requieren que otros servicios se ejecuten primero, lo que hace que se creen dependencias de los otros servicios. Otros servicios se inician solo a demanda, en lugar de hacerlo en el arranque. En ambos casos, `systemd` y `systemctl` inician los servicios según sea necesario, ya sea para resolver la dependencia o para iniciar un servicio que se usa con poca frecuencia. Por ejemplo, si el servicio de impresión (CUPS) no se está ejecutando, y se coloca un archivo en el directorio de la cola de impresión, el sistema iniciará los daemons o comandos relacionados con CUPS para ejecutar la tarea de impresión.

```
[root@host ~]# systemctl stop cups.service
Warning: Stopping cups, but it can still be activated by:
  cups.path
  cups.socket
```

Sin embargo, para detener por completo los servicios de impresión en un sistema, detenga las tres unidades. Al deshabilitar el servicio, se deshabilitarán las dependencias.

Con el comando `systemctl list-dependencies UNIT`, se visualiza una asignación de jerarquía de las dependencias para iniciar la unidad de servicio. Para enumerar dependencias inversas (unidades que dependen de la unidad especificada), use la opción `--reverse` con el comando.

```
[root@host ~]# systemctl list-dependencies sshd.service
sshd.service
• └─system.slice
•   └─sshd-keygen.target
•     └─sshd-keygen@ecdsa.service
•     └─sshd-keygen@ed25519.service
•     └─sshd-keygen@rsa.service
•     └─sysinit.target
...output omitted...
```

Enmascarar servicios y quitar máscara de servicios

En ocasiones, es posible que los diferentes servicios instalados en su sistema entren en conflicto unos con otros. Por ejemplo, existen varios métodos para administrar los servidores de correo (servicios `postfix` y `sendmail`). Enmascarar un servicio evita que un administrador inicie accidentalmente un servicio que se encuentra en conflicto con otros. El enmascaramiento crea un enlace en los directorios de configuración que se conecta con el archivo `/dev/null`, el cual impide que el servicio se inicie. Para enmascarar un servicio, use el comando `systemctl` con la opción `mask`.

```
[root@host ~]# systemctl mask sendmail.service
Created symlink /etc/systemd/system/sendmail.service → /dev/null.
```

Luego, verifique el estado del servicio con el comando `systemctl list-unit-files`:

```
[root@host ~]# systemctl list-unit-files --type=service
UNIT FILE                                     STATE
...output omitted...
sendmail.service                               masked
...output omitted...
```

El intento de iniciar una unidad de servicio enmascarada falla y arroja la siguiente salida:

```
[root@host ~]# systemctl start sendmail.service
Failed to start sendmail.service: Unit sendmail.service is masked.
```

Use el comando `systemctl unmask` para desenmascarar la unidad de servicio.

```
[root@host ~]# systemctl unmask sendmail
Removed /etc/systemd/system/sendmail.service.
```



Importante

Usted u otro archivo de unidad pueden iniciar manualmente un servicio deshabilitado, pero no se inicia automáticamente en el arranque. Un servicio enmascarado no se inicia de forma manual ni automática.

Habilitar servicios para que se inicien o se detengán en el arranque

El inicio de un servicio en un sistema en funcionamiento no garantiza que el servicio se inicie automáticamente cuando se vuelva a arrancar el sistema. De manera similar, el detenimiento de un servicio en un sistema en funcionamiento no evita que se reinicie cuando se vuelva a arrancar el sistema. Si crea enlaces en los directorios de configuración de `systemd`, habilita la opción para que el servicio se inicie en el arranque. Puede crear o eliminar estos enlaces mediante el comando `systemctl` con la opción `enable` o `disable`.

```
[root@root ~]# systemctl enable sshd.service
Created symlink /etc/systemd/system/multi-user.target.wants/sshd.service → /usr/
lib/systemd/system/sshd.service.
```

Este comando crea un enlace simbólico desde el archivo de la unidad de servicio, normalmente en el directorio `/usr/lib/systemd/system`, que se conecta con la ubicación en el disco donde el comando `systemd` busca archivos, que se encuentran en el directorio `/etc/systemd/system/TARGETNAME.target.wants`. La habilitación de un servicio no inicia el servicio en la sesión actual. Para iniciar el servicio y habilitarlo para que se inicie automáticamente durante el arranque, ejecute los comandos `systemctl start` y `systemctl enable`, o use el comando `systemctl enable --now` equivalente.

```
[root@root ~]# systemctl enable --now sshd.service
Created symlink /etc/systemd/system/multi-user.target.wants/sshd.service → /usr/
lib/systemd/system/sshd.service.
```

Para deshabilitar el servicio para que no se inicie automáticamente, use el comando `systemctl disable` que quita el enlace simbólico creado al habilitar un servicio. La desactivación de un servicio no detiene el servicio si se está ejecutando actualmente. Para deshabilitar y detener un servicio, puede ejecutar ambos comandos `systemctl stop` y `systemctl disable`, o use el comando equivalente `systemctl disable --now`.

```
[root@host ~]# systemctl disable --now sshd.service
Removed /etc/systemd/system/multi-user.target.wants/sshd.service.
```

Para verificar si el servicio está habilitado o deshabilitado, use el comando `systemctl is-enabled`.

```
[root@host ~]# systemctl is-enabled sshd.service
enabled
```

Resumen de comandos `systemctl`

Puede iniciar y detener los servicios en un sistema en funcionamiento, y habilitarlos o deshabilitarlos para que se inicien automáticamente durante el proceso de arranque.

Comandos útiles para la gestión de servicios

Comando	Tarea
<code>systemctl status <i>UNIT</i></code>	Ver información detallada sobre el estado de una unidad.
<code>systemctl stop <i>UNIT</i></code>	Detener un servicio en un sistema en funcionamiento.
<code>systemctl start <i>UNIT</i></code>	Iniciar un servicio en un sistema en funcionamiento.
<code>systemctl restart <i>UNIT</i></code>	Reiniciar un servicio en un sistema en funcionamiento.
<code>systemctl reload <i>UNIT</i></code>	Volver a cargar el archivo de configuración de un servicio en ejecución.
<code>systemctl mask <i>UNIT</i></code>	Deshabilitar el inicio (tanto manual como durante el proceso de arranque) de un servicio.
<code>systemctl unmask <i>UNIT</i></code>	Poner un servicio enmascarado a disposición.
<code>systemctl enable <i>UNIT</i></code>	Configurar un servicio para que se inicie durante el proceso de arranque. Use la opción <code>--now</code> para iniciar también el servicio.

Comando	Tarea
<code>systemctl disable UNIT</code>	Deshabilitar el inicio de un servicio durante el proceso de arranque. Use la opción <code>--now</code> para detener también el servicio.



Referencias

Páginas del manual `systemd(1)`, `systemd.unit(5)`, `systemd.service(5)`, `systemd.socket(5)` y `systemctl(1)`

Para obtener más información, consulte el capítulo *Managing System Services with systemctl* de la *Red Hat Enterprise Linux 9 Configuring Basic System Settings Guide* en

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/configuring_basic_system_settings/index#managing-system-services-with-systemctl_configuring-basic-system-settings

► Ejercicio Guiado

Control de servicios del sistema

En este ejercicio, usará `systemctl` para detener, iniciar, reiniciar, volver a cargar, habilitar y deshabilitar un servicio gestionado por `systemd`.

Resultados

- Usar el comando `systemctl` para controlar los servicios gestionados por `systemd`.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start services-control
```

Instrucciones

- 1. Inicie sesión en la máquina servera como el usuario `student` y cambie al usuario `root`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

- 2. Reinicie y recargue el servicio `sshd` y observe los resultados.

- 2.1. Muestre el estado del servicio `sshd`. Tenga en cuenta la ID del proceso del daemon `sshd`. Presione `q` para salir del comando.

```
[root@servera ~]# systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-05-19 04:04:45 EDT; 16min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 784 (sshd)
    Tasks: 1 (limit: 10799)
   Memory: 6.6M
...output omitted...
```

- 2.2. Reinicie el servicio `sshd` y visualice el estado. En este ejemplo, el ID de proceso del daemon cambia de 784 a 1193. Presione `q` para salir del comando.

```
[root@servera ~]# systemctl restart sshd
[root@servera ~]# systemctl status sshd
● sshd.service - OpenSSH server daemon
  Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
  Active: active (running) since Thu 2022-05-19 04:21:40 EDT; 5s ago
    Docs: man:sshd(8)
          man:sshd_config(5)
  Main PID: 1193 (sshd)
    Tasks: 1 (limit: 10799)
   Memory: 1.7M
...output omitted...
```

- 2.3. Vuelva a cargar el servicio sshd y visualice el estado. La ID del proceso del daemon no se modifica. Presione q para salir del comando.

```
[root@servera ~]# systemctl reload sshd
[root@servera ~]# systemctl status sshd
● sshd.service - OpenSSH server daemon
  Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
  Active: active (running) since Thu 2022-05-19 04:21:40 EDT; 52s ago
    Docs: man:sshd(8)
          man:sshd_config(5)
  Process: 1201 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/
SUCCESS)
  Main PID: 1193 (sshd)
    Tasks: 1 (limit: 10799)
   Memory: 1.7M
...output omitted...
```

- 3. Verifique que el servicio chronyd se esté ejecutando. Presione q para salir del comando.

```
[root@servera ~]# systemctl status chronyd
● chronyd.service - NTP client/server
  Loaded: loaded (/usr/lib/systemd/system/chronyd.service; enabled; vendor
preset: enabled)
  Active: active (running) since Thu 2022-05-19 04:04:44 EDT; 19min ago
...output omitted...
```

- 4. Detenga el servicio chronyd y visualice el estado. Presione q para salir del comando.

```
[root@servera ~]# systemctl stop chronyd
[root@servera ~]# systemctl status chronyd
● chronyd.service - NTP client/server
  Loaded: loaded (/usr/lib/systemd/system/chronyd.service; enabled; vendor
preset: enabled)
  Active: inactive (dead) since Thu 2022-05-19 04:24:59 EDT; 4s ago
...output omitted...
```

```
May 19 04:24:59 servera.lab.example.com systemd[1]: Stopping NTP client/server...
May 19 04:24:59 servera.lab.example.com systemd[1]: chronyd.service: Deactivated
      successfully.
May 19 04:24:59 servera.lab.example.com systemd[1]: Stopped NTP client/server.
```

- 5. Determine si el servicio chronyd está habilitado para que se inicie en el arranque del sistema.

```
[root@servera ~]# systemctl is-enabled chronyd
enabled
```

- 6. Reinicie la máquina servera y, a continuación, visualice el estado del servicio chronyd.

```
[root@servera ~]# systemctl reboot
Connection to servera closed by remote host.
Connection to servera closed.
[student@workstation ~]$
```

Inicie sesión como el usuario student en la máquina servera y cambie al usuario root. Visualice el estado del servicio chronyd. Presione q para salir del comando.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]# systemctl status chronyd
● chronyd.service - NTP client/server
  Loaded: loaded (/usr/lib/systemd/system/chronyd.service; enabled; vendor
  preset: enabled)
    Active: active (running) since Thu 2022-05-19 04:27:12 EDT; 40s ago
  ...output omitted...
```

- 7. Inhabilite el servicio chronyd para que no se inicie en el arranque del sistema y, luego, visualice el estado del servicio. Presione q para salir del comando.

```
[root@servera ~]# systemctl disable chronyd
Removed /etc/systemd/system/multi-user.target.wants/chronyd.service.
[root@servera ~]# systemctl status chronyd
● chronyd.service - NTP client/server
  Loaded: loaded (/usr/lib/systemd/system/chronyd.service; disabled; vendor
  preset: enabled)
    Active: active (running) since Thu 2022-05-19 04:27:12 EDT; 2min 48s ago
  ...output omitted...
```

- 8. Reinicie servera y, a continuación, visualice el estado del servicio chronyd.

```
[root@servera ~]# systemctl reboot
Connection to servera closed by remote host.
Connection to servera closed.
[student@workstation ~]$
```

Inicie sesión con el usuario **student** en **servera** y visualice el estado del servicio **chronyd**. Presione **q** para salir del comando.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ systemctl status chronyd
● chronyd.service - NTP client/server
  Loaded: loaded (/usr/lib/systemd/system/chronyd.service; disabled; vendor
  preset: enabled)
    Active: inactive (dead)
      Docs: man:chronyd(8)
            man:chrony.conf(5)
```

- 9. Regrese al sistema **workstation** como el usuario **student**.

```
[student@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$
```

Finalizar

En la máquina **workstation**, cambie al directorio de inicio de usuario **student** y use el comando **lab** para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish services-control
```

Esto concluye la sección.

Selección del objetivo de arranque

Objetivos

Describir el proceso de arranque de Red Hat Enterprise Linux, configurar el objetivo predeterminado que se usa en el arranque e iniciar un sistema con un objetivo no predeterminado.

Descripción del proceso de arranque de Red Hat Enterprise Linux 9

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, se requieren muchas piezas de hardware y software que funcionen en conjunto. En la siguiente lista, se proporciona una descripción general de alto nivel de las tareas de arranque de un sistema físico x86_64 de Red Hat Enterprise Linux 9. La lista de máquinas virtuales x86_64 es prácticamente la misma, pero el hipervisor maneja algunos de los pasos específicos del hardware en el software.

- La máquina se enciende. El firmware del sistema (UEFI moderno o BIOS anterior) ejecuta una *prueba automática de encendido* (*Power On Self Test, POST*) y comienza a inicializar el hardware.

Se ajusta por medio de las pantallas de configuración de BIOS o 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.

- El firmware del sistema busca un dispositivo con capacidad 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 o UEFI.

Se ajusta por medio de las pantallas de configuración de BIOS o 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.

- 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 de Red Hat Enterprise Linux 9, el cargador de arranque es *GRand Unified Bootloader versión 2* (*GRUB2*).

Se configura con el comando `grub2-install`, el cual instala GRUB2 como el cargador de arranque en el disco para sistemas BIOS. No use el comando `grub2-install` directamente para instalar el cargador de arranque de UEFI. RHEL 9 proporciona un archivo `/boot/efi/EFI/redhat/grubx64.efi` precompilado, que contiene las firmas de autenticación requeridas para un sistema de arranque seguro. La ejecución de `grub2-install` directamente en un sistema UEFI genera un nuevo archivo `grubx64.efi` sin las firmas requeridas. Puede restaurar el archivo `grubx64.efi` correcto del paquete `grub2-efi`.

- GRUB2 carga su configuración desde el archivo `/boot/grub2/grub.cfg` para BIOS y desde el archivo `/boot/efi/EFI/redhat/grub.cfg` para UEFI y muestra un menú donde puede seleccionar qué kernel arrancar.

Se configura por medio del directorio `/etc/grub.d/` y el archivo `/etc/default/grub`; el comando `grub2-mkconfig` genera los archivos `/boot/grub2/grub.cfg` o `/boot/efi/EFI/redhat/grub.cfg` para BIOS o UEFI respectivamente.

- Después de seleccionar un kernel, o después de que el tiempo de espera finaliza, el cargador de arranque carga el kernel e `initramfs` desde el disco y los coloca en la memoria. Un `initramfs` es una colección de archivos que contiene módulos del kernel para todo el hardware necesario en el arranque, scripts de inicialización y más. En Red Hat Enterprise Linux 9, `initramfs` contiene un sistema totalmente usable por sí solo.

Se configura por medio del directorio `/etc/dracut.conf.d/`, el comando `dracut` y el comando `lsinitrd` para inspeccionar el archivo `initramfs`.

- El cargador de arranque pasa el control 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.

Se configura por medio del directorio `/etc/grub.d/`, el archivo `/etc/default/grub` y el comando `grub2-mkconfig` para generar el archivo `/boot/grub2/grub.cfg`.

- El kernel inicializa todo el hardware para el que puede encontrar un controlador en el `initramfs` y, luego, ejecuta `/sbin/init` desde `initramfs` como PID 1. En Red Hat Enterprise Linux 9, `/sbin/init` es un enlace a `systemd`.

Se configura por medio del parámetro de la línea de comandos `init=` del kernel.

- La instancia `systemd` del `initramfs` ejecuta todas las unidades para el objetivo `initrd.target`. Esto incluye el montaje del sistema de archivos root en el disco en el directorio `/sysroot`.

Se configura con el archivo `/etc/fstab`.

- El kernel cambia (articula) el sistema de archivos root desde `initramfs` al sistema de archivos root en el directorio `/sysroot`. A continuación, `systemd` vuelve a ejecutarse usando la copia de `systemd` instalada en el disco.
- `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. Básicamente, un objetivo `systemd` es un conjunto de unidades que el sistema debe activar para alcanzar un estado deseado. Por lo general, estos objetivos inician una pantalla de inicio de sesión basado en texto o inicio de sesión gráfico.

Se configura con el archivo `/etc/systemd/system/default.target` y el directorio `/etc/systemd/system/`.

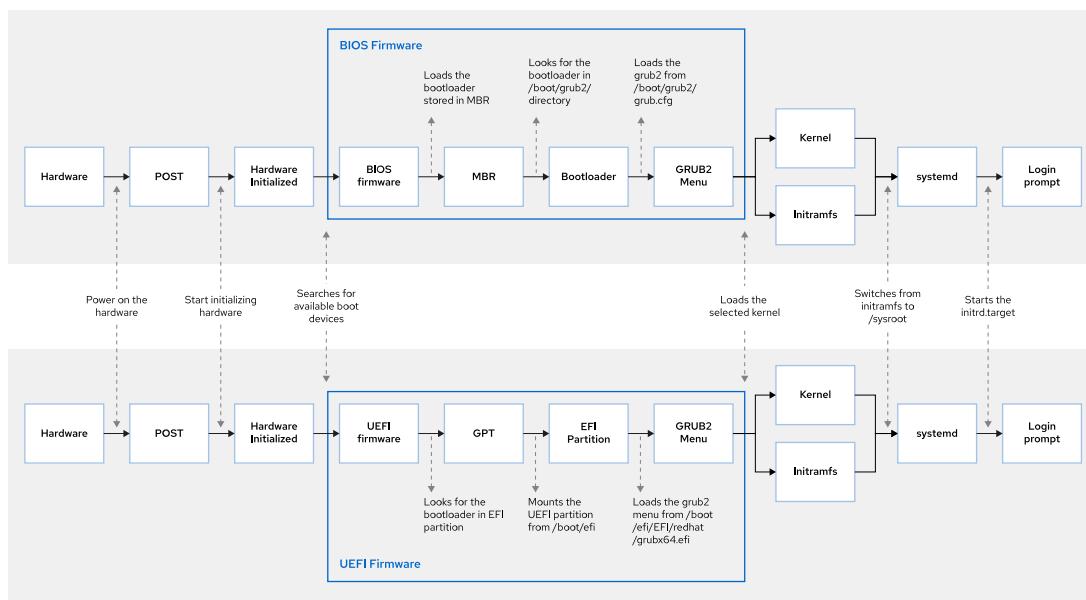


Figura 11.1: Proceso de arranque para sistemas basados en BIOS y UEFI

Reinicio y apagado

Para apagar o reiniciar un sistema en ejecución desde la línea de comandos, puede usar el comando `systemctl`.

El comando `systemctl poweroff` detiene todos los servicios en ejecución, desmonta todos los sistemas de archivos (o vuelve a montarlos como solo lectura cuando no se puedan desmontar) y, luego, apaga el sistema.

El comando `systemctl reboot` detiene todos los servicios en ejecución, desmonta todos los sistemas de archivos y, luego, reinicia el sistema.

También puede usar el atajo de estos comandos, `poweroff` y `reboot`, que son enlaces simbólicos a sus equivalentes de `systemctl`.



nota

Los comandos `systemctl halt` y `halt` también están disponibles para detener el sistema, pero a diferencia del comando `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 el sistema debe iniciar para alcanzar un estado deseado. En la siguiente tabla, se detallan los objetivos más importantes.

Objetivos que se usan normalmente

Objetivo	Propósito
<code>graphical.target</code>	El sistema soporta varios usuarios, e inicios de sesión gráficos y basados en texto.

Objetivo	Propósito
multi-user.target	El sistema soporta varios usuarios y solo inicios de sesión basados en texto.
rescue.target	Prompt <code>sulogin</code> , inicialización del sistema básica finalizada.
emergency.target	Prompt <code>sulogin</code> , cambio de <code>initramfs</code> completo y root de sistema montado en / con acceso de solo lectura.

Un objetivo puede ser parte de otro objetivo. Por ejemplo, `graphical.target` incluye `multi-user.target`, que a su vez depende de `basic.target` y otros. Puede ver estas dependencias con el siguiente comando.

```
[user@host ~]$ systemctl list-dependencies graphical.target | grep target
graphical.target
* └─multi-user.target
*   ├─basic.target
*   | ├─paths.target
*   | ├─slices.target
*   | ├─sockets.target
*   | ├─sysinit.target
*   | | ├─cryptsetup.target
*   | | ├─integritysetup.target
*   | | ├─local-fs.target
...output omitted...
```

Para enumerar los objetivos disponibles, use el siguiente comando.

```
[user@host ~]$ systemctl list-units --type=target --all
UNIT                  LOAD     ACTIVE    SUB      DESCRIPTION
-----                -----    -----    -----
basic.target          loaded   active    active  active Basic System
...output omitted...
cloud-config.target   loaded   active    active  active Cloud-config availability
cloud-init.target     loaded   active    active  active Cloud-init target
cryptsetup-pre.target (Pre)    loaded   inactive  dead    Local Encrypted Volumes
cryptsetup.target      loaded   active    active  active Local Encrypted Volumes
...output omitted...
```

Selección de un objetivo en el tiempo de ejecución

En un sistema en ejecución, los administradores pueden cambiar a un objetivo diferente con el comando `systemctl isolate`.

```
[root@host ~]# systemctl isolate multi-user.target
```

Si aísla un objetivo, detiene todos los servicios no requeridos por ese objetivo (y sus dependencias) e inicia todos los servicios requeridos que aún no se hayan iniciado.

No todos los objetivos se pueden aislar. Solo puede aislar objetivos que tengan `AllowIsolate=yes` establecido en sus archivos de unidad. Por ejemplo, puede aislar el objetivo gráfico (graphical target), pero no el objetivo `cryptsetup`.

```
[user@host ~]$ systemctl cat graphical.target
# /usr/lib/systemd/system/graphical.target
...output omitted...
[Unit]
Description=Graphical Interface
Documentation=man:systemd.special(7)
Requires=multi-user.target
Wants=display-manager.service
Conflicts=rescue.service rescue.target
After=multi-user.target rescue.service rescue.target display-manager.service
AllowIsolate=yes
[user@host ~]$ systemctl cat cryptsetup.target
# /usr/lib/systemd/system/cryptsetup.target
...output omitted...
[Unit]
Description=Local Encrypted Volumes
Documentation=man:systemd.special(7)
```

Configuración de un objetivo predeterminado

Cuando el sistema se inicia, `systemd` activa el objetivo `default.target`. Normalmente, el objetivo predeterminado en `/etc/systemd/system/` es un enlace simbólico a los objetivos `graphical.target` o `multi-user.target`. En lugar de editar este enlace simbólico manualmente, el comando `systemctl` viene con dos subcomandos para administrar este enlace: `get-default` y `set-default`.

```
[root@host ~]# systemctl get-default
multi-user.target
[root@host ~]# systemctl set-default graphical.target
Removed /etc/systemd/system/default.target.
Created symlink /etc/systemd/system/default.target → /usr/lib/systemd/system/
graphical.target.
[root@host ~]# systemctl get-default
graphical.target
```

Selección de un objetivo diferente en el momento del arranque

Para seleccionar un objetivo diferente en el momento del arranque, agregue la opción `systemd.unit=target.target` a la línea de comandos del kernel desde el cargador de arranque.

Por ejemplo, para iniciar el sistema en una shell de recuperación donde pueda cambiar la configuración del sistema sin casi ningún servicio en ejecución, agregue la siguiente opción a la línea de comandos del kernel desde el cargador de arranque.

```
systemd.unit=rescue.target
```

Este cambio de configuración solo afecta 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:

1. Arranque o reinicie el sistema.
2. Interrumpa la cuenta regresiva del menú del cargador de arranque presionando cualquier tecla (excepto **Enter** que iniciaría un arranque normal).
3. Mueva el cursor hasta la entrada del kernel que desea iniciar.
4. Presione **e** para editar la entrada actual.
5. Mueva el cursor hasta la línea que comienza con `linux`. Esta es la línea de comandos del kernel.
6. Anexe `systemd.unit=target.target`. Por ejemplo,
`systemd.unit=emergency.target`.
7. Presione **Ctrl+x** para realizar el arranque con estos cambios.



Referencias

`info grub2 (GNU GRUB manual)`

Páginas del manual: `bootup(7)`, `dracut.bootup(7)`, `lsinitrd(1)`,
`systemd.target(5)`, `systemd.special(7)`, `sulogin(8)` y `systemctl(1)`

Para obtener más información, consulte el capítulo *Managing services with systemd* de la guía *Configuring basic system settings* en
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/configuring_basic_system_settings/index#managing-services-with-systemd

► Ejercicio Guiado

Selección del objetivo de arranque

En este ejercicio, determinará el objetivo predeterminado en el que se inicia un sistema y arrancará ese sistema en otros objetivos.

Resultados

- Actualizar el objetivo predeterminado del sistema y usar un objetivo temporal desde el cargador de arranque.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start boot-selecting
```

Instrucciones

- 1. En la máquina `workstation`, abra un terminal y confirme que el objetivo predeterminado sea `graphical.target`.

```
[student@workstation ~]$ systemctl get-default
graphical.target
```

- 2. En la máquina `workstation`, cambie al objetivo `multi-user` manualmente sin reiniciar. Use el comando `sudo` y, si se le solicita, use `student` como la contraseña.

```
[student@workstation ~]$ sudo systemctl isolate multi-user.target
[sudo] password for student: student
```

- 3. Acceda a una consola basada en texto. Use la secuencia de teclas `Ctrl+Alt+F1` por medio de la entrada del menú o el botón relevantes. Inicie sesión con el usuario `root` con la contraseña `redhat`.



nota

Recordatorio: si está usando el terminal a través de una página web, puede hacer clic en el ícono Show Keyboard (Mostrar teclado) debajo de la barra de URL de su explorador web y luego a la derecha de la dirección IP de la máquina.

```
workstation login: root
Password: redhat
[root@workstation ~]#
```

- 4. Configure la máquina **workstation** para que inicie automáticamente en el objetivo **multi-user** y, luego, reinicie la máquina **workstation** para verificarlo. Cuando haya finalizado, cambie el objetivo **systemd** predeterminado al objetivo **graphical** nuevamente.

- 4.1. Establezca el objetivo predeterminado.

```
[root@workstation ~]# systemctl set-default multi-user.target
Removed /etc/systemd/system/default.target.
Created symlink /etc/systemd/system/default.target -> /usr/lib/systemd/system/
multi-user.target.
```

- 4.2. Reinicie la máquina **workstation**. Después del reinicio, el sistema presenta una consola basada en texto, no una pantalla de inicio de sesión gráfico.

```
[root@workstation ~]# systemctl reboot
```

- 4.3. Inicie sesión con el usuario **root**.

```
workstation login: root
Password: redhat
Last login: Thu Mar 28 14:50:53 on tty1
[root@workstation ~]#
```

- 4.4. Establezca el objetivo **systemd** predeterminado nuevamente en el objetivo **graphical**.

```
[root@workstation ~]# systemctl set-default graphical.target
Removed /etc/systemd/system/default.target.
Created symlink /etc/systemd/system/default.target -> /usr/lib/systemd/system/
graphical.target.
```

- 5. En esta segunda parte del ejercicio, practicará el modo de recuperación para recuperar el sistema.

Reinicie **workstation** nuevamente para acceder al cargador de arranque. Desde el menú del cargador de arranque, arranque en el objetivo **rescue** (recuperación).

- 5.1. Active el reinicio.

```
[root@workstation ~]# systemctl reboot
```

- 5.2. Cuando el menú del cargador de arranque aparezca, presione cualquier tecla (excepto **Enter** que iniciaría un arranque normal) para interrumpir la cuenta regresiva.

- 5.3. Use las teclas de dirección para destacar la entrada del cargador de arranque predeterminada.
- 5.4. Presione **e** para editar la entrada actual.
- 5.5. Con las teclas de dirección, navegue hacia la línea que comienza con `linux`.
- 5.6. Presione **End** (Fin) para mover el cursor hasta el final de la línea.
- 5.7. Agregue `systemd.unit=rescue.target` en el final de la línea.
- 5.8. Presione **Ctrl+x** para realizar el arranque con la configuración modificada.
- 5.9. Inicie sesión en el modo de recuperación. Es posible que tenga que presionar **Enter** (**Intro**) para obtener un prompt limpio.

```
Give root password for maintenance
(or press Control-D to continue): redhat
[root@workstation ~]#
```

- 6. Confirme que, en el modo de recuperación, el sistema de archivos root se encuentre en el modo de lectura y escritura.

```
[root@workstation ~]# mount
...output omitted...
/dev/vda4 on / type xfs
(rw,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota)
...output omitted...
```

- 7. Presione **Ctrl+d** para continuar con el proceso de arranque.
El sistema presenta un inicio de sesión gráfico. Inicie sesión con el usuario **student**.

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish boot-selecting
```

Esto concluye la sección.

Restablecimiento de la contraseña de root

Objetivos

Iniciar sesión en un sistema y cambiar la contraseña de root cuando la actual se haya perdido.

Restablecimiento de la contraseña de root desde el cargador de arranque.

Una tarea que todos los administradores de sistemas deben ser capaces de realizar es restablecer una contraseña `root` perdida. Si el administrador aún tiene la sesión iniciada, ya sea como usuario no privilegiado, pero con acceso sudo completo, o como `root`, esta tarea es sencilla. Esta tarea es un poco más complicada cuando el administrador no ha iniciado sesión.

Existen muchos métodos para establecer una nueva contraseña `root`. Un administrador de sistemas podría, por ejemplo, arrancar el sistema usando un Live CD, montar el sistema de archivos `root` desde allí y editar `/etc/shadow`. En esta sección, exploramos un método que no requiere el uso de medios externos.



nota

En Red Hat Enterprise Linux 6 y en las versiones anteriores, los administradores pueden arrancar el sistema en el nivel de ejecución 1 para obtener un prompt de `root`. Los análogos más cercanos al nivel de ejecución 1 en una máquina Red Hat Enterprise Linux 8 o posterior son los objetivos de recuperación y emergencia y ambos requieren la contraseña `root` para iniciar sesión.

Si su sistema se implementó desde una imagen de nube de Red Hat, no tendrá un kernel de rescate en su menú de arranque; sin embargo, su kernel predeterminado tendrá un comportamiento similar que le permitirá ingresar al modo de mantenimiento sin la contraseña de `root`.

En Red Hat Enterprise Linux 9, es posible tener scripts que se ejecuten desde la pausa de `initramfs` en ciertos puntos, proporcionar una shell `root` y, luego, continuar cuando esa shell se cierre. Esto se suele realizar principalmente para depuraciones, pero también se puede usar para restablecer una contraseña `root` perdida.

A partir de Red Hat Enterprise Linux 9, si instala su sistema desde un DVD, el kernel predeterminado solicita la contraseña `root` cuando intenta ingresar al modo de mantenimiento. Por lo tanto, para restablecer una contraseña `root` perdida, debe usar el kernel de rescate. No obstante, si implementa su sistema desde una imagen de nube de Red Hat, no tiene un kernel de rescate en su menú de arranque, pero su kernel predeterminado presenta un comportamiento similar que le permite ingresar al modo de mantenimiento sin la contraseña `root`.

Para acceder a la shell `root`, siga estos pasos:

1. Reinicie el sistema.
2. Interrumpa la cuenta regresiva del cargador de arranque presionando cualquier tecla (excepto `Enter`).

3. Mueva el cursor a la entrada del kernel de rescate para arrancar (la que tiene la palabra `rescue` en su nombre).
4. Presione `e` para editar la entrada seleccionada.
5. Mueva el cursor hasta la línea de comandos del kernel (la línea que empieza con `linux`).
6. Anexe `rd.break`. Con esa opción, se produce un quiebre en el sistema antes de que el control se entregue de `initramfs` al sistema real.
7. Presione `Ctrl+x` para realizar el arranque con los cambios.
8. Presione `Enter` para realizar el mantenimiento cuando se le solicite.

En este punto, se presenta una shell `root`, con el sistema de archivos root real en el disco montado para solo lectura en `/sysroot`. Debido a que la solución de problemas suele exigir modificaciones en el sistema de archivos root, debe volver a montar el sistema de archivos root para que su acceso sea de lectura y escritura. En el siguiente paso, se muestra cómo la opción `remount, rw` del comando `mount` vuelve a montar el sistema de archivos con la opción nueva (`rw`) configurada.



nota

Es posible que las imágenes compiladas previamente coloquen múltiples argumentos `console=` en el kernel para respaldar una amplia variedad de situaciones de implementación. Estos argumentos `console=` indican los dispositivos que se deben usar para la salida por consola. La advertencia con `rd.break` es que si bien el sistema envía los mensajes del kernel a todas las consolas, el prompt usará en última instancia la última consola. Si no recibe el prompt, es posible que desee reordenar temporalmente los argumentos `console=` cuando edite la línea de comandos del kernel desde el cargador de arranque.



Importante

El sistema aún no ha habilitado SELinux, por lo que cualquier archivo que cree no tiene contexto SELinux. Algunas herramientas, como el comando `passwd`, primero crean un archivo temporal, y, luego, lo reemplazan con el archivo que intentan editar; y se crea así de manera efectiva un nuevo archivo sin un contexto SELinux. Por este motivo, cuando usa el comando `passwd` con `rd.break`, el archivo `/etc/shadow` no recibe un contexto SELinux.

Para restablecer la contraseña `root` desde este punto, realice el siguiente procedimiento:

1. Vuelva a montar `/sysroot` con acceso de lectura y escritura.

```
sh-5.1# mount -o remount,rw /sysroot
```

2. Cambie a jail de `chroot`, donde `/sysroot` se trata como la root de un árbol de sistemas de archivos.

```
sh-5.1# chroot /sysroot
```

3. Establezca una nueva contraseña `root`.

```
sh-5.1# passwd root
```

- Asegúrese de que todos los archivos no etiquetados, incluido /etc/shadow en este punto, obtengan una nueva etiqueta durante el arranque.

```
sh-5.1# touch /.autorelabel
```

- Ingrese exit dos veces. El primer comando saldrá del jail de chroot y el segundo comando saldrá de la shell de depuración de initramfs.

En este punto, el sistema continúa con el arranque, realiza un nuevo etiquetado de SELinux completo y, luego, realiza el arranque nuevamente.

Inspección de registros

Puede ser útil mirar los registros de arranques anteriores que fallaron. Si los diarios (journals) del sistema son persistentes durante los reinicios, puede usar la herramienta journalctl para inspeccionar esos registros.

Recuerde que, de manera predeterminada, los diarios (journals) del sistema se almacenan en el directorio /run/log/journal, lo que significa que se borran cuando se reinicia el sistema. Para almacenar diarios (journals) en el directorio /var/log/journal, que no se borra en los reinicios, configure el parámetro Storage en persistent en /etc/systemd/journald.conf.

```
[root@host ~]# vim /etc/systemd/journald.conf
...
[Journal]
Storage=persistent
...
[root@host ~]# systemctl restart systemd-journald.service
```

Para inspeccionar los registros de un arranque anterior, use la opción -b del comando journalctl. Sin ningún argumento, la opción -b del comando journalctl solo muestra mensajes desde el último arranque. Si el argumento es un número negativo, se muestran los registros de los arranques anteriores.

```
[root@host ~]# journalctl -b -1 -p err
```

Este comando muestra todos los mensajes calificados como error o peor del arranque anterior.

Reparación de problemas de arranque de Systemd

Para solucionar problemas de inicio del servicio en el momento del arranque, Red Hat Enterprise Linux 8 y posteriores cuentan con las siguientes herramientas.

Habilitación de la shell de depuración temprana

Al habilitar el servicio debug-shell con systemctl enable debug-shell.service, el sistema genera una shell root en TTY9 (Ctrl+Alt+F9) al principio de la secuencia de arranque. Esta shell inicia sesión automáticamente como root, de modo que los administradores pueden depurar el sistema mientras el sistema operativo aún está arrancando.

**Advertencia**

No olvide deshabilitar el servicio `debug-shell.service` cuando haya finalizado la depuración, ya que deja una shell `root` no autenticada abierta a cualquier usuario con acceso a la consola local.

O bien puede seguir estos pasos para activar la shell de depuración durante el arranque con el menú de GRUB2:

1. Reinicie el sistema.
2. Interrumpa la cuenta regresiva del cargador de arranque presionando cualquier tecla (excepto `Enter`).
3. Mueva el cursor hasta la entrada del kernel que debe iniciarse.
4. Presione `e` para editar la entrada seleccionada.
5. Mueva el cursor hasta la línea de comandos del kernel (la línea que empieza con `linux`).
6. Anexe `systemd.debug-shell`. Con este parámetro, el sistema arranca en la shell de depuración.
7. Presione `Ctrl+x` para realizar el arranque con los cambios.

Uso de los 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 indica una shell de emergencia o recuperación 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 el objetivo de recuperación espera que `sysinit.target` se complete, para que una mayor parte del sistema se inicie (p. ej., servicio de inicio de sesión o sistemas de archivos). El usuario `root` en este punto no puede hacer cambios a `/etc/fstab` hasta que la unidad se vuelva a montar en un estado de lectura y escritura con el comando `mount -o remount, rw /`.

Los administradores pueden usar estas shells para corregir 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.

Identificación de trabajos atascados

Durante el inicio, `systemd` inicia una cantidad de trabajos. Si alguno de estos trabajos no se puede completar, impide que se ejecuten otros trabajos. Para inspeccionar la lista de trabajos actual, los administradores pueden 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)`, `journald.conf(5)`, `journalctl(1)` y `systemctl(1)`

► Ejercicio Guiado

Restablecimiento de la contraseña de root

En este ejercicio, restablece la contraseña `root` en un sistema.

Resultados

- Restablecer una contraseña de usuario de `root` perdida.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando ejecuta un script de inicio que determina si la máquina `servera` es accesible en la red. También restablece la contraseña `root` a una cadena aleatoria y establece un tiempo de espera mayor para el menú de GRUB2.

```
[student@workstation ~]$ lab start boot-resetting
```

Instrucciones

- ▶ 1. Vuelva a arrancar `servera` e interrumpa la cuenta regresiva en el menú del cargador de arranque.
 - 1.1. Localice el ícono de la consola de `servera`, según corresponda para el entorno del aula y, luego, abra la consola.
Envíe `Ctrl+Alt+Del` a su sistema usando la entrada del menú o el botón relevantes.
 - 1.2. Cuando el menú del cargador de arranque aparezca, presione cualquier tecla (excepto `Enter`) para interrumpir la cuenta regresiva.
- ▶ 2. Edite la entrada del cargador de arranque del kernel de rescate (en la memoria) para anular el proceso de arranque después de que todos los sistemas de archivos hayan sido montados por el kernel, pero antes de que el control se entregue a `systemd`.
 - 2.1. Use las teclas del cursor para resaltar la entrada del kernel de rescate (la que tiene la palabra `rescue` en su nombre).
 - 2.2. Presione `e` para editar la entrada actual.
 - 2.3. Use las teclas de dirección para navegar hacia la línea que comienza con `linux`.
 - 2.4. Presione `End` (Fin) para mover el cursor hasta el final de la línea.
 - 2.5. Agregue `rd.break` en el final de la línea.
 - 2.6. Presione `Ctrl+x` para realizar el arranque con la configuración modificada.

- 3. Presione **Enter** para realizar el mantenimiento. En el prompt **sh-5.1#**, vuelva a montar el sistema de archivos **/sysroot** con acceso de lectura y escritura y, luego, use el comando **chroot** para ingresar a un jail **chroot** en **/sysroot**.

```
sh-5.1# mount -o remount,rw /sysroot  
...output omitted...  
sh-5.1# chroot /sysroot
```

- 4. Cambie la contraseña **root** a **redhat**.

```
sh-5.1# passwd root  
Changing password for user root.  
New password: redhat  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password: redhat  
passwd: all authentication tokens updated successfully.
```

- 5. Configure el sistema para que realice automáticamente un etiquetado nuevo de SELinux completo después del arranque. Esto es necesario porque el comando **passwd** recrea el archivo **/etc/shadow** sin un contexto SELinux.

```
sh-5.1# touch /.autorelabel
```

- 6. Escriba **exit** dos veces para continuar reiniciando su sistema de forma habitual. El sistema ejecuta una operación de reetiquetado de SELinux y, luego, se reinicia automáticamente. Cuando el sistema esté funcionando, verifique su trabajo al iniciar sesión como **root** en la consola.

Finalizar

En la máquina **workstation**, cambie al directorio de inicio de usuario **student** y use el comando **lab** para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish boot-resetting
```

Esto concluye la sección.

Reparación de problemas del sistema de archivos en el arranque

Objetivos

Reparar manualmente la configuración del sistema de archivos o problemas de daños que detengan el proceso de arranque.

Problemas del sistema de archivos

Durante el proceso de arranque, el servicio `systemd` monta los sistemas de archivos persistentes definidos en el archivo `/etc/fstab`.

Los errores en el archivo `/etc/fstab` o los sistemas de archivos dañados pueden impedir que un sistema complete el proceso de arranque. En algunos escenarios de falla, el sistema sale del proceso de arranque y abre una shell de emergencia que requiere la contraseña de usuario `root`.

La siguiente lista describe algunos problemas comunes de montaje del sistema de archivos al analizar `/etc/fstab` durante el proceso de arranque:

Sistema de archivos dañado

El servicio `systemd` intenta reparar el sistema de archivos. Si el problema no se puede reparar automáticamente, el sistema abre una shell de emergencia.

Dispositivo o UUID no existente

El tiempo de espera del servicio `systemd` se agota esperando que el dispositivo esté disponible. Si el dispositivo no responde, el sistema abre una shell de emergencia.

Punto de montaje no existente o incorrecto

El sistema abre una shell de emergencia.

Reparación de problemas del sistema de archivos

Para obtener acceso a un sistema que no puede completar el arranque debido a problemas del sistema de archivos, la arquitectura `systemd` proporciona un objetivo de arranque `emergency`, que abre una shell de emergencia que requiere la contraseña `root` para acceder.

El siguiente ejemplo demuestra la salida del proceso de arranque cuando el sistema encuentra un problema del sistema de archivos y cambia al objetivo `emergency`:

```
...output omitted...
[*      ] A start job is running for /dev/vda2 (27s / 1min 30s)
[ TIME ] Timed out waiting for device /dev/vda2.
[DEPEND] Dependency failed for /mnt/mountfolder
[DEPEND] Dependency failed for Local File Systems.
[DEPEND] Dependency failed for Mark need to relabel after reboot.
...output omitted...
[ OK    ] Started Emergency Shell.
[ OK    ] Reached target Emergency Mode.
...output omitted...
Give root password for maintenance
(or press Control-D to continue):
```

capítulo 11 | Servicios de control y proceso de arranque

El daemon `systemd` no pudo montar el dispositivo `/dev/vda2` y se agotó el tiempo de espera. Debido a que el dispositivo no está disponible, el sistema abre una shell de emergencia para el acceso de mantenimiento.

Para reparar problemas del sistema de archivos cuando su sistema abre una shell de emergencia, primero localice el sistema de archivos errante, determine y repare la falla, luego vuelva a cargar la configuración '`systemd`' para volver a intentar el montaje automático.

Use el comando `mount` para determinar qué sistemas de archivos están montados actualmente por el daemon `systemd`.

```
[root@host ~]# mount  
...output omitted...  
/dev/vda1 on / type xfs (ro,relatime,seclabel,attr2,inode64,noquota)  
...output omitted...
```

Si el sistema de archivos root se monta con la opción `ro` (solo lectura), usted no podrá editar el archivo `/etc/fstab`. Vuelva a montar temporalmente el sistema de archivos root con la opción `rw` (lectura y escritura), si es necesario, antes de abrir el archivo `/etc/fstab`. La opción de volver a montar permite que un sistema de archivos en uso modifique sus parámetros de montaje sin tener que desmontar el sistema de archivos.

```
[root@host ~]# mount -o remount,rw /
```

Intente montar todos los sistemas de archivos enumerados en el archivo `/etc/fstab` con la opción `mount --all`. Esta opción monta procesos en cada entrada del sistema de archivos, pero omite los que ya están montados. El comando muestra los errores que ocurren al montar un sistema de archivos.

```
[root@host ~]# mount --all  
mount: /mnt/mountfolder: mount point does not exist.
```

En este escenario, el directorio de montaje `/mnt/mountfolder` no existe; cree el directorio `/mnt/mountfolder` antes de volver a intentar el montaje. Pueden aparecer otros mensajes de error, incluidos errores tipográficos en las entradas o nombres de dispositivos o UUID incorrectos.

Cuando haya corregido todos los problemas en el archivo `/etc/fstab`, informe al daemon `systemd` para que registre el nuevo archivo `/etc/fstab` con el comando `systemctl daemon-reload`, luego intente montar todas las entradas.

```
[root@host ~]# systemctl daemon-reload  
[root@host ~]# mount --all
```



nota

El servicio `systemd` procesa el archivo `/etc/fstab` transformando cada entrada en una configuración de unidad `systemd` tipo `.mount` y, luego, inicie la unidad como un servicio. `daemon-reload` solicita a que `systemd` vuelva a compilar y a cargar todas las configuraciones de unidad.

Si el intento `mount --all` se ejecuta correctamente sin más errores, la prueba final es verificar que el montaje del sistema de archivos se realiza correctamente durante el arranque del sistema. Reinicie el sistema y espere a que el arranque finalice normalmente.

```
[root@host ~]# systemctl reboot
```

Para realizar pruebas rápidas en el archivo `/etc/fstab`, use la opción de entrada de montaje `nofail`. Usar la opción `nofail` en una entrada `/etc/fstab` permite que el sistema arranque, incluso si el montaje de ese sistema de archivos no se ejecuta de forma correcta. Esta opción no debe usarse con sistemas de archivos de producción que siempre deben montarse. Con la opción `nofail`, una aplicación se podría iniciar sin los datos del sistema de archivos y generar posibles consecuencias graves.



Referencias

Páginas del manual: `systemd-fsck(8)`, `systemd-fstab-generator(8)` y `systemd.mount(5)`

► Ejercicio Guiado

Reparación de problemas del sistema de archivos en el arranque

En este ejercicio, recuperará un sistema de una configuración incorrecta en el archivo `/etc/fstab` que hace que falle el proceso de arranque.

Resultados

- Diagnosticar problemas del archivo `/etc/fstab` y usar el modo de emergencia para recuperar el sistema.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start boot-repairing
```

Instrucciones

- 1. Acceda a la consola de la máquina `servera` y observe que el proceso de arranque no se ejecuta correctamente desde el principio.
 1. Localice el ícono de la consola de `servera`, según corresponda para el entorno del aula. Abra la consola.
Advierta que, al parecer, un trabajo de inicio no se ejecuta por completo. Tómese un momento para especular sobre la posible causa de este comportamiento.
 2. Reinicie la máquina `servera` al enviar un `Ctrl+Alt+Del` a su sistema usando la entrada del menú o el botón relevantes. En el caso de este problema de arranque en particular, esta secuencia de teclas podría no detener inmediatamente el trabajo en ejecución y es posible que tenga que esperar a que finalice el tiempo de espera antes de que el sistema se reinicie.
Si espera a que la tarea finalice el tiempo de espera sin enviar `Ctrl+Alt+Del`, el sistema eventualmente genera por su cuenta una shell de emergencia.
 3. Cuando el menú del cargador de arranque aparezca, presione cualquier tecla (excepto `Enter`) para interrumpir la cuenta regresiva.
- 2. Si observa el error que tuvo en el arranque anterior, parece que al menos ciertas partes del sistema aún están funcionando. Use `redhat` como contraseña de usuario `root` para intentar un arranque de emergencia.
 1. Use las teclas de dirección para destacar la entrada del cargador de arranque predeterminada.

- 2.2. Presione la tecla **e** para editar la entrada actual.
- 2.3. Use las teclas de dirección para navegar hacia la línea que comienza con la palabra **linux**.
- 2.4. Presione **End** (Fin) para mover el cursor hasta el final de la línea.
- 2.5. Agregue la cadena **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.

```
Give root password for maintenance
(or press Control-D to continue): redhat
[root@servera ~]#
```

► 4. Determine qué sistemas de archivos está montando el daemon **systemd** actualmente. Observe que el daemon **systemd** monta el sistema de archivos root en modo de solo lectura.

```
[root@servera ~]# mount
...output omitted...
/dev/vda4 on / type xfs
(ro,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota)
...output omitted...
```

► 5. Vuelva a montar el sistema de archivos root en modo de lectura y escritura.

```
[root@servera ~]# mount -o remount,rw /
```

► 6. Intente montar todos los demás sistemas de archivos. La opción **--all (-a)** monta todos los sistemas de archivos detallados en el archivo **/etc/fstab** que todavía no están montados.

```
[root@servera ~]# mount -a
mount: /RemoveMe: mount point does not exist.
```

► 7. Edite el archivo **/etc/fstab** para corregir el problema.

7.1. Elimine o comente la línea incorrecta con el comando **vim /etc/fstab**.

```
[root@servera ~]# cat /etc/fstab
...output omitted...
# /dev/sdz1  /RemoveMe  xfs  defaults  0 0
```

7.2. Vuelva a cargar el daemon **systemd** para que el sistema registre la nueva configuración del archivo **/etc/fstab**.

```
[root@servera ~]# systemctl daemon-reload
```

- 8. Intente montar todas las entradas para verificar que el archivo /etc/fstab ahora sea correcto.

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

- 9. Reinicie el sistema y espere a que el arranque finalice. Ahora el sistema debería arrancar normalmente.

```
[root@servera ~]# systemctl reboot
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish boot-repairing
```

Esto concluye la sección.

► Trabajo de laboratorio

Control del proceso de arranque

En este trabajo de laboratorio, restablece la contraseña de `root` en un sistema, corrige una configuración incorrecta y establece el objetivo de arranque predeterminado.

Resultados

- Restablecer una contraseña perdida para el usuario `root`.
- Diagnosticar y corregir problemas de arranque.
- Establecer el objetivo `systemd` predeterminado.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start boot-review
```

Instrucciones

1. En la máquina `serverb`, restablezca la contraseña a `redhat` para el usuario `root`. Localice el ícono de la consola de la máquina `serverb`, según corresponda para el entorno del aula y, luego, abra la consola.
2. En el menú del cargador de arranque, seleccione la entrada predeterminada del cargador de arranque del kernel. El sistema no puede arrancar porque un trabajo de inicio no se completa correctamente. Corrija el problema desde la consola de la máquina `serverb`.
3. Cambie el objetivo de `systemd` predeterminado en la máquina `serverb` para que el sistema inicie automáticamente una interfaz gráfica en el arranque.
No hay una interfaz gráfica instalada en la máquina `serverb`. Solo establezca el objetivo predeterminado para este ejercicio y no instale los paquetes.

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade boot-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish boot-review
```

Esto concluye la sección.

► Solución

Control del proceso de arranque

En este trabajo de laboratorio, restablece la contraseña de `root` en un sistema, corrige una configuración incorrecta y establece el objetivo de arranque predeterminado.

Resultados

- Restablecer una contraseña perdida para el usuario `root`.
- Diagnosticar y corregir problemas de arranque.
- Establecer el objetivo `systemd` predeterminado.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start boot-review
```

Instrucciones

1. En la máquina `serverb`, restablezca la contraseña a `redhat` para el usuario `root`. Localice el ícono de la consola de la máquina `serverb`, según corresponda para el entorno del aula y, luego, abra la consola.
 - 1.1. Envíe `Ctrl+Alt+Del` a su sistema usando la entrada del menú o el botón relevantes.
 - 1.2. Cuando el menú del cargador de arranque aparezca, presione cualquier tecla (excepto `Enter`) para interrumpir la cuenta regresiva.
 - 1.3. Use las teclas del cursor para resaltar la entrada del cargador de arranque del kernel de rescate (la que tiene la palabra `rescue` en su nombre).
 - 1.4. Presione `e` para editar la entrada actual.
 - 1.5. Use las teclas de dirección para navegar por la línea que comienza con el texto `linux`.
 - 1.6. Presione `Ctrl+e` (Fin) para mover el cursor hasta el final de la línea.
 - 1.7. Agregue el texto `rd.break` en el final de la línea.
 - 1.8. Presione `Ctrl+x` para realizar el arranque con la configuración modificada.
 - 1.9. Presione `Enter` para ingresar al modo de mantenimiento.
 - 1.10. En el prompt `sh-5.1`, vuelva a montar el sistema de archivos `/sysroot` en modo escritura, luego use el comando `chroot` para el directorio `/sysroot`.

```
sh-5.1# mount -o remount,rw /sysroot
...output omitted...
sh-5.1# chroot /sysroot
```

- 1.11. Establezca **redhat** como contraseña para el usuario **root**.

```
sh-5.1# passwd root
Changing password for user root.
New password: redhat
BAD PASSWORD: The password is shorter than 8 characters
Retype new password: redhat
passwd: all authentication tokens updated successfully.
```

- 1.12. Configure el sistema para que realice automáticamente un etiquetado nuevo de SELinux completo después del arranque.

```
sh-5.1# touch /.autorelabel
```

- 1.13. Salga del entorno **chroot** y del prompt **sh-5.1**. Después de volver a etiquetar el sistema de archivos, el sistema solicita ingresar al modo de mantenimiento, pero si espera, completa el reinicio y muestra el menú del cargador de arranque.
2. En el menú del cargador de arranque, seleccione la entrada predeterminada del cargador de arranque del kernel. El sistema no puede arrancar porque un trabajo de inicio no se completa correctamente. Corrija el problema desde la consola de la máquina **serverb**.
 - 2.1. Arranque el sistema en modo de emergencia. Reinicie la máquina **serverb** al enviar un **Ctrl+Alt+Del** a su sistema usando la entrada del menú o el botón relevantes.
 - 2.2. Cuando el menú del cargador de arranque aparezca, presione cualquier tecla (excepto **Enter**) para interrumpir la cuenta regresiva.
 - 2.3. Use las teclas de dirección para destacar la entrada predeterminada del cargador de arranque.
 - 2.4. Presione **e** para editar la entrada actual.
 - 2.5. Use las teclas de dirección para navegar por la línea que comienza con el texto **linux**.
 - 2.6. Presione **Ctrl+e** (Fin) para mover el cursor hasta el final de la línea.
 - 2.7. Agregue el texto **systemd.unit=emergency.target** en el final de la línea.
 - 2.8. Presione **Ctrl+x** para realizar el arranque con la configuración modificada.
 - 2.9. Inicie sesión en el modo de emergencia.

```
Give root password for maintenance
(or press Control-D to continue): redhat
[root@serverb ~]#
```

- 2.10. Vuelva a montar el sistema de archivos / en modo escritura.

```
[root@serverb ~]# mount -o remount,rw /
...output omitted...
```

- 2.11. Monte todos los sistemas de archivos.

```
[root@serverb ~]# mount -a
mount: /olddata: can't find UUID=4d5c85a5-8921-4a06-8aff-80567e9689bc.
```

- 2.12. Edite el archivo `/etc/fstab` para eliminar o comentar la línea incorrecta que monta el punto de montaje `/olddata`.

```
[root@serverb ~]# vim /etc/fstab
...output omitted...
#UUID=4d5c85a5-8921-4a06-8aff-80567e9689bc  /olddata  xfs  defaults  0 0
```

- 2.13. Actualice el daemon `systemd` para que el sistema registre los cambios en la configuración del archivo `/etc/fstab`.

```
[root@serverb ~]# systemctl daemon-reload
```

- 2.14. Intente montar todas las entradas para verificar que la configuración del archivo `/etc/fstab` sea correcto.

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

- 2.15. Reinicie el sistema y espere a que el arranque finalice. Ahora el sistema debería arrancar normalmente.

```
[root@serverb ~]# systemctl reboot
```

3. Cambie el objetivo de `systemd` predeterminado en la máquina `serverb` para que el sistema inicie automáticamente una interfaz gráfica en el arranque.

No hay una interfaz gráfica instalada en la máquina `serverb`. Solo establezca el objetivo predeterminado para este ejercicio y no instale los paquetes.

- 3.1. Inicie sesión en la máquina `servera` como el usuario `student` y cambie al usuario `root`.

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
[student@serverb ~]$ sudo -i
[sudo] password for student: student
[root@serverb ~]#
```

- 3.2. Establezca `graphical.target` como el objetivo predeterminado.

```
[root@serverb ~]# systemctl set-default graphical.target
Removed /etc/systemd/system/default.target.
Created symlink /etc/systemd/system/default.target → /usr/lib/systemd/system/
graphical.target.
```

3.3. Verifique que esté configurado el valor predeterminado correcto.

```
[root@serverb ~]# systemctl get-default
graphical.target
```

3.4. Regrese a la máquina `workstation` como el usuario `student`.

```
[root@serverb ~]# exit
logout
[student@serverb ~]$ exit
logout
Connection to serverb closed.
```

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade boot-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish boot-review
```

Esto concluye la sección.

Resumen

- Se usa `systemctl` para iniciar, detener, volver a cargar, habilitar y deshabilitar servicios.
- Use la utilidad `systemd` para administrar unidades de servicio, unidades de socket y unidades de ruta.
- Use el comando `systemctl status` para determinar el estado de los daemons del sistema y los servicios de red iniciados por `systemd`.
- El comando `systemctl list-dependencies` enumera todas las unidades de servicio de las que depende una unidad de servicio específica.
- La utilidad `systemd` puede enmascarar una unidad de servicio para que no se ejecute ni siquiera para dar respuesta a las dependencias.
- Los comandos `systemctl reboot` y `systemctl poweroff` reinician y apagan el sistema, respectivamente.
- El comando `systemctl isolate target-name.target` cambia a un nuevo objetivo en tiempo de ejecución.
- Los comandos `systemctl get-default` y `systemctl set-default` se usan para consultar y establecer el objetivo predeterminado.
- La opción `rd.break` en la línea de comandos del kernel interrumpe el proceso de arranque antes de que se entregue el control desde el sistema de archivos initramfs. El sistema de archivos root se monta como solo lectura en el directorio `/sysroot`.
- El objetivo de emergencia contribuye a diagnosticar y corregir problemas de sistemas de archivos.

capítulo 12

Analizar y almacenar registros

Meta

Ubicar e interpretar correctamente registros de eventos del sistema para la resolución de problemas.

Objetivos

- Describir la arquitectura básica de registro que emplea Red Hat Enterprise Linux para registrar eventos
- Interpretar eventos en archivos syslog relevantes a los fines de resolver problemas o revisar el estado del sistema
- Buscar e interpretar entradas en el diario (journal) del sistema para resolver problemas o revisar el estado del sistema
- Configurar el diario (journal) del sistema para resguardar el registro de eventos cuando se reinicia un servidor
- Mantener una sincronización de hora precisa por medio del Protocolo de Tiempo de la Red (NTP) y configurar la zona horaria para garantizar marcas de tiempo correctas para los eventos registrados por el diario (journal) y los registros del sistema.

Secciones

- Descripción de la arquitectura de registro del sistema (y cuestionario)
- Revisión de archivos syslog (y ejercicio guiado)
- Revisión de entradas del diario (journal) del sistema (y ejercicio guiado)
- Resguardo del diario (journal) del sistema (y ejercicio guiado)
- Mantenimiento de la hora correcta (y ejercicio guiado)

Trabajo de laboratorio

Analizar y almacenar registros

Descripción de la arquitectura de registro del sistema

Objetivos

Describir la arquitectura básica de registro que emplea Red Hat Enterprise Linux para registrar eventos

Registro del sistema

El kernel del sistema operativo y otros procesos llevan un registro de los eventos que suceden cuando el sistema está ejecutándose. Estos registros se usan para realizar una auditoría del sistema y solucionar problemas. Puede usar utilidades de texto como los comandos `less` y `tail` para inspeccionar estos registros.

Red Hat Enterprise Linux usa un sistema de registro estándar que se basa en el protocolo Syslog para registrar los mensajes del sistema. Muchos programas usan el sistema de registro para registrar eventos y organizarlos en archivos de registro. Los servicios `systemd-journald` y `rsyslog` se encargan de gestionar los mensajes de syslog en Red Hat Enterprise Linux 9.

El servicio `systemd-journald` está en el corazón de la arquitectura de registro de eventos del sistema operativo. El servicio `systemd-journald` recopila mensajes de eventos de muchas fuentes:

- Kernel del sistema
- Salida de las primeras etapas del proceso de arranque
- Salida estándar y error estándar de daemons
- Eventos de syslog

El servicio `systemd-journald` reestructura los registros en un formato estándar y los escribe en un diario (journal) de sistema indexado y estructurado. De forma predeterminada, este diario (journal) se almacena en un sistema de archivos que no persiste en los reinicios.

Sin embargo, el servicio `rsyslog` lee los mensajes de syslog recibidos por el servicio `systemd-journald` desde el diario (journal) a medida que llegan. El servicio `rsyslog` procesa los eventos de syslog, los registra en sus archivos de registro o los reenvía a otros servicios de acuerdo con su propia configuración.

El servicio `rsyslog` ordena y escribe mensajes de syslog en los archivos de registro que no persisten en los reinicios en el directorio `/var/log`. El servicio también clasifica los mensajes de registro en archivos de registro específicos según el tipo de programa que envió cada mensaje y la prioridad de cada mensaje de syslog.

Además de los archivos de mensajes de syslog, el directorio `/var/log` contiene archivos de registro de otros servicios en el sistema. En la siguiente tabla, se enumeran algunos archivos útiles del directorio `/var/log`.

Archivos de registro del sistema seleccionados

Archivo de registro	Tipo de mensajes almacenados
/var/log/messages	La mayoría de los mensajes de syslog se registran aquí. Las excepciones incluyen mensajes relacionados con tareas de autenticación y procesamiento de correos electrónicos, con ejecución de trabajos programados y aquellos relacionados exclusivamente con tareas de depuración.
/var/log/secure	Mensajes de syslog relacionados con eventos de seguridad y autenticación.
/var/log/maillog	Mensajes de syslog relacionados con el servidor de correo.
/var/log/cron	Mensajes de syslog relacionados con la ejecución de trabajos programados.
/var/log/boot.log	Mensajes de la consola que no son de syslog relacionados con el inicio del sistema.

Algunas aplicaciones no usan el servicio `syslog` para administrar sus mensajes de registro. Por ejemplo, el servidor web Apache guarda los mensajes de registro en archivos en un subdirectorio del directorio `/var/log`.



Referencias

Páginas del manual: `systemd-journald.service(8)`, `rsyslogd(8)` y `rsyslog.conf(5)`

Para obtener más información, consulte la sección *Troubleshooting Problems Using Log Files* en *Red Hat Enterprise Linux 9 Configuring Basic System Settings Guide* en https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/configuring_basic_system_settings/index

► Cuestionario

Descripción de la arquitectura de registro del sistema

Elija la respuesta correcta para las siguientes preguntas:

- ▶ 1. **¿Qué archivo de registro almacena la mayoría de los mensajes de syslog, excepto los relacionados con la autenticación, el correo, los trabajos programados y la depuración?**
 - a. /var/log/maillog
 - b. /var/log/boot.log
 - c. /var/log/messages
 - d. /var/log/secure
- ▶ 2. **¿Qué archivo de registro almacena los mensajes de syslog relacionados con las operaciones de seguridad y autenticación en el sistema?**
 - a. /var/log/maillog
 - b. /var/log/boot.log
 - c. /var/log/messages
 - d. /var/log/secure
- ▶ 3. **¿Qué servicio ordena y organiza los mensajes de syslog en archivos en /var/log?**
 - a. rsyslog
 - b. systemd-journald
 - c. auditd
 - d. tuned
- ▶ 4. **¿Qué directorio contiene los archivos de syslog legibles?**
 - a. /sys/kernel/debug
 - b. /var/log/journal
 - c. /run/log/journal
 - d. /var/log
- ▶ 5. **¿Qué archivo almacena mensajes de syslog relacionados con el servidor de correo?**
 - a. /var/log/lastlog
 - b. /var/log/maillog
 - c. /var/log/tallylog
 - d. /var/log/boot.log

- ▶ 6. ¿Qué archivo almacena mensajes de syslog relacionados con los trabajos programados?
 - a. /var/log/cron
 - b. /var/log/tallylog
 - c. /var/log/spooler
 - d. /var/log/secure

- ▶ 7. ¿Qué archivo almacena mensajes de la consola relacionados con el inicio del sistema?
 - a. /var/log/messages
 - b. /var/log/cron
 - c. /var/log/boot.log
 - d. /var/log/secure

► Solución

Descripción de la arquitectura de registro del sistema

Elija la respuesta correcta para las siguientes preguntas:

- ▶ 1. **¿Qué archivo de registro almacena la mayoría de los mensajes de syslog, excepto los relacionados con la autenticación, el correo, los trabajos programados y la depuración?**
 - a. /var/log/maillog
 - b. /var/log/boot.log
 - c. /var/log/messages
 - d. /var/log/secure
- ▶ 2. **¿Qué archivo de registro almacena los mensajes de syslog relacionados con las operaciones de seguridad y autenticación en el sistema?**
 - a. /var/log/maillog
 - b. /var/log/boot.log
 - c. /var/log/messages
 - d. /var/log/secure
- ▶ 3. **¿Qué servicio ordena y organiza los mensajes de syslog en archivos en /var/log?**
 - a. rsyslog
 - b. systemd-journald
 - c. auditd
 - d. tuned
- ▶ 4. **¿Qué directorio contiene los archivos de syslog legibles?**
 - a. /sys/kernel/debug
 - b. /var/log/journal
 - c. /run/log/journal
 - d. /var/log
- ▶ 5. **¿Qué archivo almacena mensajes de syslog relacionados con el servidor de correo?**
 - a. /var/log/lastlog
 - b. /var/log/maillog
 - c. /var/log/tallylog
 - d. /var/log/boot.log

- ▶ 6. ¿Qué archivo almacena mensajes de syslog relacionados con los trabajos programados?
 - a. /var/log/cron
 - b. /var/log/tallylog
 - c. /var/log/spooler
 - d. /var/log/secure

- ▶ 7. ¿Qué archivo almacena mensajes de la consola relacionados con el inicio del sistema?
 - a. /var/log/messages
 - b. /var/log/cron
 - c. /var/log/boot.log
 - d. /var/log/secure

Revisión de archivos Syslog

Objetivos

Interpretar eventos en archivos syslog relevantes a los fines de resolver problemas o revisar el estado del sistema

Registro de eventos en el sistema

Muchos programas usan el protocolo syslog para registrar eventos en el sistema. Cada mensaje se clasifica por instalación (qué subsistema produce el mensaje) y prioridad (gravedad del mensaje).

En la siguiente tabla, se enumeran las instalaciones de syslog estándar.

Descripción general de las instalaciones de syslog

Código	Instalación	Descripción de la instalación
0	kern	Mensajes del kernel
1	user	Mensajes de nivel de usuario
2	mail	Mensajes del sistema de correo
3	daemon	Mensajes de daemons del sistema
4	auth	Mensajes de autenticación y seguridad
5	syslog	Mensajes de syslog internos
6	lpr	Mensajes de la impresora
7	news	Mensajes de noticias de la red
8	uucp	Mensajes del protocolo UUCP
9	cron	Mensajes del daemon de reloj
10	authpriv	Mensajes de autorización ajenos al sistema
11	ftp	Mensajes de protocolo FTP
16-23	local0 to local7	Mensajes locales personalizados

En la siguiente tabla, se enumeran las prioridades estándar de syslog de mayor a menor.

Descripción general de las prioridades de syslog

Código	Prioridad	Descripción de la prioridad
0	emerg	El sistema no se puede usar

Código	Prioridad	Descripción de la prioridad
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 `rsyslog` usa la instalación y la prioridad de los mensajes de registro para determinar cómo resolverlos. Las reglas configuran esta utilidad y prioridad en el archivo `/etc/rsyslog.conf` y en cualquier archivo en el directorio `/etc/rsyslog.d` con la extensión `.conf`. Los paquetes de software pueden agregar reglas fácilmente instalando un archivo apropiado en el directorio `/etc/rsyslog.d`.

Cada regla que controla cómo ordenar los mensajes de `syslog` tiene una línea en uno de los archivos de configuración. En el lado izquierdo de cada línea, se indican la instalación y la gravedad del mensaje de `syslog` que se corresponde con la regla. En el lado derecho de cada línea, se indica en qué archivo se debe guardar el mensaje de registro (o a dónde más enviar el mensaje). Un asterisco (*) es un comodín que coincide con todos los valores.

Por ejemplo, la siguiente línea en el archivo `/etc/rsyslog.d` registraría los mensajes enviados a la instalación `authpriv` en cualquier prioridad para el archivo `/var/log/secure`:

```
authpriv.*          /var/log/secure
```

En ocasiones, los mensajes de registro a veces coinciden con más de una regla en el archivo `rsyslog.conf`. En estos casos, un mensaje se almacena en más de un archivo de registro. Para limitar los mensajes almacenados, la palabra clave `none` en el campo de prioridad señala que no se deben almacenar mensajes para la instalación indicada en el archivo dado.

En lugar de registrarse en un archivo, también pueden imprimirse en las terminales de todos los usuarios que hayan iniciado sesión. El archivo `rsyslog.conf` tiene una configuración para imprimir todos los mensajes de `syslog` con la prioridad `emerg` en las terminales de todos los usuarios que hayan iniciado sesión.

Reglas de muestra del servicio `rsyslog`

```
##### 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 subsistema de syslog tiene muchas más características que no se incluyen en este curso. Para explorar más a fondo, consulte la página del manual `rsyslog.conf(5)` y la extensa documentación HTML en `/usr/share/doc/rsyslog/html/index.html` que proporciona el paquete `rsyslog-doc`.

Rotación del archivo de registro

El comando `logrotate` rota los archivos de registro para evitar que ocupen demasiado espacio en el directorio `/var/log`. Cuando se rota un archivo de registro, se le cambia el nombre con una extensión que indica la fecha de rotación. Por ejemplo, el antiguo archivo `/var/log/messages` se renombra al archivo `/var/log/messages-20220320` cuando se rota el 2022-03-20. Después de que el archivo de registro anterior rota, crea un archivo de registro y notifica al servicio que escribió el archivo de registro.

Después de una determinada cantidad de rotaciones, durante cuatro semanas, el archivo de registro más viejo se descarta para liberar espacio en disco. Un trabajo programado ejecuta el comando `logrotate` diariamente para ver el requisito de rotación de los archivos de registro. La mayoría de los archivos de registro rotan semanalmente; el comando `logrotate` rota algunos archivos de registro más rápido o más lentamente, o cuando alcanzan un tamaño específico.

Análisis de una entrada de syslog

Los mensajes de registro comienzan con el mensaje más antiguo al principio y el mensaje más nuevo al final del archivo de registro. El servicio `rsyslog` usa un formato estándar al registrar las entradas en los archivos de registro. En el siguiente ejemplo, se explica la anatomía de un mensaje de registro en el archivo de registro `/var/log/secure`.

```
Mar 20 20:11:48 localhost sshd[1433]: Failed password for student from 172.25.0.10
port 59344 ssh2
```

- **Mar 20 20:11:48**: Registra la marca de tiempo de la entrada de registro.
- **localhost**: Host que envía el mensaje de registro.

- **sshd[1433]** : Nombre del programa o el proceso y el número de PID que envió el mensaje de registro.
- **Failed password for ...** : Mensaje que se envió.

Monitorear eventos de registro

Para reproducir problemas, es útil monitorear 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 en el archivo.

Por ejemplo, para monitorear los intentos fallidos de inicio de sesión, ejecute el comando `tail` en un terminal y, luego, en otro terminal, ejecute el comando `ssh` como el usuario `root` mientras un usuario intenta iniciar sesión en el sistema.

En el primer terminal, ejecute el comando `tail`:

```
[root@host ~]# tail -f /var/log/secure
```

En el segundo terminal, ejecute el comando `ssh`:

```
[root@host ~]# ssh root@hosta
root@hosta's password: redhat
...output omitted...
[root@hostA ~]#
```

Los mensajes de registro están visibles en el primer terminal.

```
...output omitted...
Mar 20 09:01:13 host sshd[2712]: Accepted password for root from 172.25.254.254
port 56801 ssh2
Mar 20 09:01:13 host sshd[2712]: pam_unix(sshd:session): session opened for user
root by (uid=0)
```

Envío manual de mensajes de syslog

El comando `logger` envía mensajes al servicio `rsyslog`. De manera predeterminada, envía el mensaje al tipo de usuario con la prioridad `notice` (`user.notice`) prioridad, a menos que se especifique lo contrario con la opción `-p`. Es útil probar los cambios en la configuración del servicio `rsyslog`.

Para enviar un mensaje al servicio `rsyslog` que se graba en el archivo de registro `/var/log/boot.log`, ejecute el siguiente comando `logger`:

```
[root@host ~]# logger -p local7.notice "Log entry created on host"
```



Referencias

Páginas del manual: `logger(1)`, `tail(1)`, `rsyslog.conf(5)` y `logrotate(8)`

Manual de `rsyslog`

- `/usr/share/doc/rsyslog/html/index.html` provisto por el paquete `rsyslog-doc`

Para obtener más información, consulte *Troubleshooting Problems Using Log Files* en

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/configuring_basic_system_settings/assembly_troubleshooting_problems-using-log-files_configuring-basic-system-settings

► Ejercicio Guiado

Revisión de archivos Syslog

En este ejercicio, volverá a configurar el servicio `rsyslog` para escribir mensajes de registro específicos en un archivo nuevo.

Resultados

- Configurar el servicio `rsyslog` para escribir todos los mensajes de registro con la prioridad `debug` en el archivo de registro `/var/log/messages-debug`.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start logs-syslog
```

Instrucciones

- 1. Inicie sesión en la máquina `servera` como el usuario `student` y cambie al usuario `root`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

- 2. Configure el servicio `rsyslog` en la máquina `servera` para registrar todos los mensajes con la prioridad `debug`, o una prioridad más elevada, para cualquier servicio en un archivo de registro `/var/log/messages-debug` nuevo al cambiar el archivo de configuración `/etc/rsyslog.d/debug.conf`.

- 2.1. Cree el archivo `/etc/rsyslog.d/debug.conf` con las entradas necesarias para redirigir todos los mensajes de registro con prioridad `debug` al archivo de registro `/var/log/messages-debug`.

```
* .debug /var/log/messages-debug
```

Esta línea de configuración captura los mensajes de syslog con cualquier tipo y un nivel de prioridad `debug` o superior. El servicio `rsyslog` escribe esos mensajes que coinciden en el archivo de registro `/var/log/messages-debug`. El comodín (*) en los campos de tipo o prioridad de la línea de configuración indica cualquier tipo o prioridad de los mensajes de registros.

- 2.2. Reinicie el servicio `rsyslog`.

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

- 3. Verifique que todos los mensajes de registro con prioridad debug aparezcan en el archivo de registro /var/log/messages-debug.

- 3.1. Genere un mensaje de registro con el tipo user y la prioridad debug.

```
[root@servera ~]# logger -p user.debug "Debug Message Test"
```

- 3.2. Vea los últimos diez mensajes de registro del archivo de registro /var/log/messages-debug y confirme que visualiza el mensaje Debug Message Test entre los otros mensajes de registro.

```
[root@servera ~]# tail /var/log/messages-debug
Feb 13 18:22:38 servera systemd[1]: Stopping System Logging Service...
Feb 13 18:22:38 servera rsyslogd[25176]: [origin software="rsyslogd"
  swVersion="8.37.0-9.el8" x-pid="25176" x-info="http://www.rsyslog.com"] exiting
  on signal 15.
Feb 13 18:22:38 servera systemd[1]: Stopped System Logging Service.
Feb 13 18:22:38 servera systemd[1]: Starting System Logging Service...
Feb 13 18:22:38 servera rsyslogd[25410]: environment variable TZ is not set, auto
  correcting this to TZ=/etc/localtime [v8.37.0-9.el8 try http://www.rsyslog.com/
  e/2442 ]
Feb 13 18:22:38 servera systemd[1]: Started System Logging Service.
Feb 13 18:22:38 servera rsyslogd[25410]: [origin software="rsyslogd"
  swVersion="8.37.0-9.el8" x-pid="25410" x-info="http://www.rsyslog.com"] start
Feb 13 18:27:58 servera student[25416]: Debug Message Test
```

- 3.3. Regrese al sistema workstation como el usuario student.

```
[root@servera ~]# exit
logout
[student@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$
```

Finalizar

En la máquina workstation, cambie al directorio de inicio de usuario student y use el comando lab para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish logs-syslog
```

Esto concluye la sección.

Revisión de las entradas del diario (journal) del sistema

Objetivos

Buscar e interpretar entradas en el diario (journal) del sistema para resolver problemas o revisar el estado del sistema

Buscar eventos en el diario (journal) del sistema

El servicio `systemd-journald` almacena datos de registro en un archivo binario estructurado e indexado, que se denomina *diario (journal)*. Estos datos incluyen información adicional sobre el evento de registro. Por ejemplo, para los eventos de `syslog`, esta información incluye la prioridad del mensaje original y la *instalación*, que es un valor que el servicio `syslog` asigna para rastrear el proceso que originó un mensaje.



Importante

En Red Hat Enterprise Linux, el directorio `/run/log` basado en la memoria almacena el diario (journal) del sistema de forma predeterminada. El contenido del directorio `/run/log` se pierde cuando se apaga el sistema. Puede cambiar el directorio `journald` a una ubicación persistente, que se analiza más adelante en este capítulo.

Para recuperar mensajes de registro del diario (journal), use el comando `journalctl`. Puede usar el comando `journalctl` para ver todos los mensajes en el diario (journal) o para buscar eventos específicos basados en una amplia gama de opciones y criterios. Si ejecuta el comando como `root`, tiene acceso completo al diario (journal). Los usuarios normales también pueden usar el comando `journalctl`, pero se les puede restringir la visualización de ciertos mensajes.

```
[root@host ~]# journalctl
...output omitted...
Mar 15 04:42:16 host.lab.example.com systemd[2127]: Listening on PipeWire
Multimedia System Socket.
Mar 15 04:42:16 host.lab.example.com systemd[2127]: Starting Create User's
Volatile Files and Directories...
Mar 15 04:42:16 host.lab.example.com systemd[2127]: Listening on D-Bus User
Message Bus Socket.
Mar 15 04:42:16 host.lab.example.com systemd[2127]: Reached target Sockets.
Mar 15 04:42:16 host.lab.example.com systemd[2127]: Finished Create User's
Volatile Files and Directories.
Mar 15 04:42:16 host.lab.example.com systemd[2127]: Reached target Basic System.
Mar 15 04:42:16 host.lab.example.com systemd[1]: Started User Manager for UID 0.
Mar 15 04:42:16 host.lab.example.com systemd[2127]: Reached target Main User
Target.
Mar 15 04:42:16 host.lab.example.com systemd[2127]: Startup finished in 90ms.
Mar 15 04:42:16 host.lab.example.com systemd[1]: Started Session 6 of User root.
Mar 15 04:42:16 host.lab.example.com sshd[2110]: pam_unix(sshd:session): session
opened for user root(uid=0) by (uid=0)
```

capítulo 12 | Analizar y almacenar registros

```
Mar 15 04:42:17 host.lab.example.com systemd[1]: Starting Hostname Service...
Mar 15 04:42:17 host.lab.example.com systemd[1]: Started Hostname Service.
lines 1951-2000/2000 (END) q
```

El comando `journalctl` destaca los mensajes de registro importantes: los mensajes con prioridad `notice` o `warning` se muestran en negrita, y los mensajes con prioridad `error` o una prioridad mayor se muestran en rojo.

La clave para usar en forma correcta el diario (journal) para la solución de problemas y auditorías es limitar las búsquedas en el diario para mostrar solo la salida relevante.

De manera predeterminada, el comando `journalctl` con la opción `-n` muestra las 10 últimas entradas de registro. Puede ajustar la cantidad de entradas de registro con un argumento opcional que especifique cuántas entradas de registro se mostrarán. Por ejemplo, si desea revisar las últimas cinco entradas de registro, puede ejecutar el siguiente comando `journalctl`:

```
[root@host ~]# journalctl -n 5
Mar 15 04:42:17 host.lab.example.com systemd[1]: Started Hostname Service.
Mar 15 04:42:47 host.lab.example.com systemd[1]: systemd-hostnamed.service:
  Deactivated successfully.
Mar 15 04:47:33 host.lab.example.com systemd[2127]: Created slice User Background
  Tasks Slice.
Mar 15 04:47:33 host.lab.example.com systemd[2127]: Starting Cleanup of User's
  Temporary Files and Directories...
Mar 15 04:47:33 host.lab.example.com systemd[2127]: Finished Cleanup of User's
  Temporary Files and Directories.
```

Al igual que el comando `tail`, el comando `journalctl` con la opción `-f` ofrece las últimas 10 líneas del diario (journal) del sistema y continúa proporcionando entradas del diario nuevas a medida que se escriben en el diario. Para salir del comando `journalctl` con la opción `-f`, use la combinación de teclas `Ctrl+C`.

```
[root@host ~]# journalctl -f
Mar 15 04:47:33 host.lab.example.com systemd[2127]: Finished Cleanup of User's
  Temporary Files and Directories.
Mar 15 05:01:01 host.lab.example.com CROND[2197]: (root) CMD (run-parts /etc/
  cron.hourly)
Mar 15 05:01:01 host.lab.example.com run-parts[2200]: (/etc/cron.hourly) starting
  @anacron
Mar 15 05:01:01 host.lab.example.com anacron[2208]: Anacron started on 2022-03-15
Mar 15 05:01:01 host.lab.example.com anacron[2208]: Will run job `cron.daily' in
  29 min.
Mar 15 05:01:01 host.lab.example.com anacron[2208]: Will run job `cron.weekly' in
  49 min.
Mar 15 05:01:01 host.lab.example.com anacron[2208]: Will run job `cron.monthly' in
  69 min.
Mar 15 05:01:01 host.lab.example.com anacron[2208]: Jobs will be executed
  sequentially
Mar 15 05:01:01 host.lab.example.com run-parts[2210]: (/etc/cron.hourly) finished
  @anacron
```

capítulo 12 | Analizar y almacenar registros

```
Mar 15 05:01:01 host.lab.example.com CROND[2196]: (root) CMDEND (run-parts /etc/cron.hourly)
^C
[root@host ~]#
```

Para solucionar problemas, se recomienda filtrar el resultado del diario (journal) en función de la prioridad de las entradas del diario. El comando `journalctl` con la opción `-p` muestra las entradas del diario (journal) con un nivel de prioridad especificado (por nombre o por número) o superior. El comando `journalctl` procesa los niveles de prioridad `debug, info, notice, warning, err, crit, alert y emerg`, en orden de prioridad ascendente.

Como ejemplo, ejecute el siguiente comando `journalctl` para enumerar las entradas del diario (journal) con prioridad `err` o prioridad superior:

```
[root@host ~]# journalctl -p err
Mar 15 04:22:00 host.lab.example.com pipewire-pulse[1640]: pw.conf: execvp error
  'pactl': No such file or direct
Mar 15 04:22:17 host.lab.example.com kernel: Detected CPU family 6 model 13
  stepping 3
Mar 15 04:22:17 host.lab.example.com kernel: Warning: Intel Processor - this
  hardware has not undergone testing by Red Hat and might not be certif>
Mar 15 04:22:20 host.lab.example.com smartd[669]: DEVICESCAN failed: glob(3)
  aborted matching pattern /dev/discs/disc*
Mar 15 04:22:20 host.lab.example.com smartd[669]: In the system's table of devices
  NO devices found to scan
```

Es posible que desee mostrar mensajes para una unidad systemd específica. Puede mostrar mensajes para una unidad systemd especificada mediante el uso del comando `journalctl` con la opción `-u` y el nombre de la unidad.

```
[root@host ~]# journalctl -u sshd.service
May 15 04:30:18 host.lab.example.com systemd[1]: Starting OpenSSH server daemon...
May 15 04:30:18 host.lab.example.com sshd[1142]: Server listening on 0.0.0.0 port
  22.
May 15 04:30:18 host.lab.example.com sshd[1142]: Server listening on :: port 22.
May 15 04:30:18 host.lab.example.com systemd[1]: Started OpenSSH server daemon.
May 15 04:32:03 host.lab.example.com sshd[1796]: Accepted publickey for user1 from
  172.25.250.254 port 43876 ssh2: RSA SHA256:1UGy...>
May 15 04:32:03 host.lab.example.com sshd[1796]: pam_unix(sshd:session): session
  opened for user user1(uid=1000) by (uid=0)
May 15 04:32:26 host.lab.example.com sshd[1866]: Accepted publickey for user2
  from ::1 port 36088 ssh2: RSA SHA256:M8ik...
May 15 04:32:26 host.lab.example.com sshd[1866]: pam_unix(sshd:session): session
  opened for user user2(uid=1001) by (uid=0)
lines 1-8/8 (END) q
```

Cuando se buscan eventos específicos, puede limitar el resultado a un período específico. El comando `journalctl` tiene dos opciones para limitar el resultado a un rango de tiempo determinado, las opciones `--since` y `--until`. Ambas opciones consideran un argumento de tiempo con el formato `"DD-MM-AAAA hh:mm:ss"` (las comillas dobles son necesarias para conservar el espacio en la opción).

El comando `journalctl` asume que el día comienza a las 00:00:00 cuando omite el argumento de la hora. El comando también asume el día actual cuando omite el argumento del día. Ambas

capítulo 12 | Analizar y almacenar registros

opciones consideran `yesterday`, `today` y `tomorrow` como argumentos válidos, además del campo de fecha y hora.

Como ejemplo, ejecute el siguiente comando `journalctl` para enumerar todas las entradas del diario (journal) de los registros de hoy.

```
[root@host ~]# journalctl --since today
...output omitted...
Mar 15 05:04:20 host.lab.example.com systemd[1]: Started Session 8 of User
student.
Mar 15 05:04:20 host.lab.example.com sshd[2255]: pam_unix(sshd:session): session
opened for user student(uid=1000) by (uid=0)
Mar 15 05:04:20 host.lab.example.com systemd[1]: Starting Hostname Service...
Mar 15 05:04:20 host.lab.example.com systemd[1]: Started Hostname Service.
Mar 15 05:04:50 host.lab.example.com systemd[1]: systemd-hostnamed.service:
Deactivated successfully.
Mar 15 05:06:33 host.lab.example.com systemd[2261]: Starting Mark boot as
successful...
Mar 15 05:06:33 host.lab.example.com systemd[2261]: Finished Mark boot as
successful.
lines 1996-2043/2043 (END) q
```

Ejecute el siguiente comando `journalctl` para enumerar todas las entradas del diario (journal) que van de `2022-03-11 20:30:00` a `2022-03-14 10:00:00`.

```
[root@host ~]# journalctl --since "2022-03-11 20:30" --until "2022-03-14 10:00"
...output omitted...
```

También puede especificar todas las entradas desde un tiempo relativo al presente. Por ejemplo, para especificar todas las entradas en la última hora, puede usar el siguiente comando:

```
[root@host ~]# journalctl --since "-1 hour"
...output omitted...
```

**nota**

Puede usar otras especificaciones de tiempo más sofisticadas con las opciones `--since` y `--until`. Para algunos ejemplos, vea la página del manual `systemd.time(7)`.

Además del contenido visible del diario (journal), puede ver entradas de registro adicionales si activa la salida detallada. Para filtrar el resultado de una consulta del diario (journal), puede usarse cualquier campo adicional que se muestra. La salida verbal es útil para restringir el resultado de búsquedas complejas para determinados eventos del diario (journal).

```
[root@host ~]# journalctl -o verbose
Tue 2022-03-15 05:10:32.625470 EDT [s=e7623387430b4c14b2c71917db58e0ee;i...]
 _BOOT_ID=beaadd6e5c5448e393ce716cd76229d4
 _MACHINE_ID=4ec03abd2f7b40118b1b357f479b3112
 PRIORITY=6
 SYSLOG_FACILITY=3
 SYSLOG_IDENTIFIER=systemd
```

```
_UID=0
_GID=0
_TRANSPORT=journal
_CAP_EFFECTIVE=1fffffffffffff
TID=1
CODE_FILE=src/core/job.c
CODE_LINE=744
CODE_FUNC=job_emit_done_message
JOB_RESULT=done
_PID=1
_COMM=systemd
_EXE=/usr/lib/systemd/systemd
_SYSTEMD_CGROUP=/init.scope
_SYSTEMD_UNIT=init.scope
_SYSTEMD_SLICE=--slice
JOB_TYPE=stop
MESSAGE_ID=9d1aaa27d60140bd96365438aad20286
_HOSTNAME=host.lab.example.com
_CMDLINE=/usr/lib/systemd/systemd --switched-root --system --deserialize 31
_SELINUX_CONTEXT=system_u:system_r:init_t:s0
UNIT=user-1000.slice
MESSAGE=Removed slice User Slice of UID 1000.
INVOCATION_ID=0e5efc1b4a6d41198f0cf02116ca8aa8
JOB_ID=3220
_SOURCE_REALTIME_TIMESTAMP=1647335432625470
lines 46560-46607/46607 (END) q
```

En la siguiente lista, se muestran los campos comunes del diario (journal) del sistema que se pueden usar para buscar líneas relevantes para un proceso o evento en particular:

- *_COMM*: nombre del comando.
- *_EXE*: ruta hacia el archivo ejecutable para el proceso
- *_PID*: PID del proceso.
- *_UID*: UID del usuario que ejecuta el proceso.
- *_SYSTEMD_UNIT*: unidad `systemd` que inició el proceso

Es posible combinar más de un campo del diario (journal) del sistema para realizar una búsqueda detallada con el comando `journalctl`. Por ejemplo, el siguiente comando `journalctl` muestra todas las entradas del diario (journal) relacionadas con la unidad `sshd.service` `systemd` de un proceso con la PID 2110.

```
[root@host ~]# journalctl _SYSTEMD_UNIT=sshd.service _PID=2110
Mar 15 04:42:16 host.lab.example.com sshd[2110]: Accepted
publickey for root from 172.25.250.254 port 46224 ssh2: RSA
SHA256:1UGybTe52L2jzEJa1HLVKn9QUCKrTv3ZzxNMJol1Fro
Mar 15 04:42:16 host.lab.example.com sshd[2110]: pam_unix(sshd:session): session
opened for user root(uid=0) by (uid=0)
```



nota

Para obtener una lista de los campos más usados del diario (journal), consulte la página del manual `systemd.journal-fields(7)`.



Referencias

Páginas del manual: `journalctl(1)`, `systemd.journal-fields(7)` y `systemd.time(7)`

Para obtener más información, consulte la sección *Troubleshooting Problems Using Log Files* en *Red Hat Enterprise Linux 9 Configuring Basic System Settings Guide* en https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/configuring_basic_system_settings/index#troubleshooting-problems-using-log-files_getting-started-with-system-administration

► Ejercicio Guiado

Revisión de las entradas del diario (journal) del sistema

En este ejercicio, buscará en el diario (journal) del sistema las entradas que registren eventos que coincidan con criterios específicos.

Resultados

- Buscar en el diario (journal) del sistema las entradas que registran eventos en función de diferentes criterios.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start logs-systemd
```

Instrucciones

- 1. Desde la máquina `workstation`, abra una sesión de SSH en la máquina `servera` como el usuario `student`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

- 2. Use el comando `journalctl` con la opción `_PID=1` para mostrar solo los eventos de registro que se originan en el proceso `systemd` PID 1 en la máquina `servera`. Para salir del comando `journalctl`, presione `q`. La siguiente salida es un ejemplo y puede diferir en su sistema:

```
[student@servera ~]$ journalctl _PID=1
Mar 15 04:21:14 localhost systemd[1]: Finished Load Kernel Modules.
Mar 15 04:21:14 localhost systemd[1]: Finished Setup Virtual Console.
Mar 15 04:21:14 localhost systemd[1]: dracut ask for additional cmdline parameters
was skipped because all trigger condition checks failed.
Mar 15 04:21:14 localhost systemd[1]: Starting dracut cmdline hook...
Mar 15 04:21:14 localhost systemd[1]: Starting Apply Kernel Variables...
lines 1-5 q
[student@servera ~]$
```

capítulo 12 | Analizar y almacenar registros

- 3. Use el comando `journalctl` con la opción `_UID=81` para mostrar todos los eventos de registro que se originan de un servicio del sistema con una PID 81 en la máquina `servera`.

```
[student@servera ~]$ journalctl _UID=81
Mar 15 04:21:17 servera.lab.example.com dbus-broker-lau[727]: Ready
```

- 4. Use el comando `journalctl` con la opción `-p warning` para visualizar eventos de registro con prioridad `warning` y prioridad superior en la máquina `servera`.

```
[student@servera ~]$ journalctl -p warning
Mar 15 04:21:14 localhost kernel: wait_for_initramfs() called before
rootfs_initcalls
Mar 15 04:21:14 localhost kernel: ACPI: PRMT not present
Mar 15 04:21:14 localhost kernel: acpi PNP0A03:00: fail to add MMCONFIG
information, can't access extended PCI configuration space under this bridge.
Mar 15 04:21:14 localhost kernel: device-mapper: core: CONFIG_IMA_DISABLE_HTABLE
is disabled. Duplicate IMA measurements will not be recorded in the IMA log.
...output omitted...
Mar 15 04:21:18 servera.lab.example.com NetworkManager[769]: <warn>
[1647332478.5504] device (eth0): mtu: failure to set IPv6 MTU
Mar 15 04:21:27 servera.lab.example.com chronyd[751]: System clock wrong by
-0.919695 seconds
Mar 15 04:22:34 servera.lab.example.com chronyd[751]: System clock wrong by
0.772805 seconds
Mar 15 05:41:11 servera.lab.example.com sshd[1104]: error:
kex_exchange_identification: Connection closed by remote host
lines 1-19/19 (END) q
[student@servera ~]$
```

- 5. Muestre todos los eventos de registro registrados en los últimos 10 minutos a partir de la hora actual en la máquina `servera`.

```
[student@servera ~]$ journalctl --since "-10min"
Mar 15 05:40:01 servera.lab.example.com anacron[1092]: Job `cron.weekly' started
Mar 15 05:40:01 servera.lab.example.com anacron[1092]: Job `cron.weekly'
terminated
Mar 15 05:41:11 servera.lab.example.com sshd[1104]: error:
kex_exchange_identification: Connection closed by remote host
Mar 15 05:41:11 servera.lab.example.com sshd[1104]: Connection closed by
172.25.250.9 port 45370
Mar 15 05:41:14 servera.lab.example.com sshd[1105]: Accepted publickey for student
from 172.25.250.9 port 45372 ssh2: RSA SHA256:M8ikhcEDm2tQ95Z0o7ZvufqEixCFCT
+wowZLNzNlBT0
Mar 15 05:41:14 servera.lab.example.com systemd[1]: Created slice User Slice of
UID 1000.
Mar 15 05:41:14 servera.lab.example.com systemd[1]: Starting User Runtime
Directory /run/user/1000...
Mar 15 05:41:14 servera.lab.example.com systemd-logind[739]: New session 1 of user
student.
Mar 15 05:41:14 servera.lab.example.com systemd[1]: Finished User Runtime
Directory /run/user/1000.
Mar 15 05:41:14 servera.lab.example.com systemd[1]: Starting User Manager for UID
1000...
```

```
...output omitted...
Mar 15 05:44:56 servera.lab.example.com systemd[1109]: Stopped target Sockets.
Mar 15 05:44:56 servera.lab.example.com systemd[1109]: Stopped target Timers.
Mar 15 05:44:56 servera.lab.example.com systemd[1109]: Stopped Mark boot as
successful after the user session has run 2 minutes.
Mar 15 05:44:56 servera.lab.example.com systemd[1109]: Stopped Daily Cleanup of
User's Temporary Directories.
lines 1-48 q
[student@servera ~]$
```

- 6. Use el comando `journalctl` con las opciones `--since` y `_SYSTEMD_UNIT="sshd.service"` para visualizar todos los eventos de registro que se originan del servicio `sshd` registrado desde las `09:00:00` de esta mañana en la máquina `servera`.



nota

Las aulas en línea generalmente se ejecutan en la zona horaria UTC. Para obtener resultados que comienzan a las 9:00 a. m. en su zona horaria local, ajuste su valor, desde el valor por la cantidad de su desplazamiento de UTC. De manera alternativa, ignore la hora local y use un valor de 9:00 para ubicar las entradas del diario (journal) que ocurrieron desde las 9:00 para la zona horaria de `servera`.

```
[student@servera ~]$ journalctl --since 9:00:00 _SYSTEMD_UNIT="sshd.service"
Mar 15 09:41:14 servera.lab.example.com sshd[1105]: Accepted publickey for student
from 172.25.250.9 port 45372 ssh2: RSA SHA256:M8ikhcEDm2tQ95Z007ZvufqEixCFct
+wowZLNzNlBT0
Mar 15 09:41:15 servera.lab.example.com sshd[1105]: pam_unix(sshd:session):
session opened for user student(uid=1000) by (uid=0)
Mar 15 09:44:56 servera.lab.example.com sshd[1156]: Accepted publickey for student
from 172.25.250.9 port 45374 ssh2: RSA SHA256:M8ikhcEDm2tQ95Z007ZvufqEixCFct
+wowZLNzNlBT0
Mar 15 09:44:56 servera.lab.example.com sshd[1156]: pam_unix(sshd:session):
session opened for user student(uid=1000) by (uid=0)
```

- 7. Regrese al sistema `workstation` como el usuario `student`.

```
[student@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish logs-systemd
```

Esto concluye la sección.

Resguardo del diario (journal) del sistema

Objetivos

Configurar el diario (journal) del sistema para resguardar el registro de eventos cuando se reinicia un servidor

Almacenamiento del diario (journal) del sistema

De manera predeterminada, Red Hat Enterprise Linux 9 almacena el diario (journal) del sistema en el directorio `/run/log`, y el sistema borra el diario del sistema después de un reinicio. Puede cambiar los ajustes de configuración del servicio `systemd-journald` en el archivo `/etc/systemd/journald.conf` para hacer que los diarios (journals) no se borren en el reinicio.

El parámetro `Storage` en el archivo `/etc/systemd/journald.conf` define si desea almacenar los diarios (journals) del sistema de forma volátil o de forma persistente durante el reinicio.

Establezca este parámetro en `persistent`, `volatile`, `auto` o `none` de la siguiente manera:

- `persistent`: almacena los diarios (journals) en el directorio `/var/log/journal`, que no se borra en los reinicios. Si el directorio `/var/log/journal` no existe, el servicio `systemd-journald` lo crea.
- `volatile`: almacena los diarios (journals) en el directorio `/run/log/journal` volátil. Puesto que el sistema de archivos `/run` es temporal y solo existe en la memoria de tiempo de ejecución, los datos almacenados en él, incluidos los diarios (journals) del sistema, se borran en el reinicio.
- `auto`: si el directorio `/var/log/journal` existe, el servicio `systemd-journald` usa el almacenamiento persistente; de lo contrario, usa el almacenamiento volátil. Esta acción es la predeterminada si no establece el parámetro `Storage`.
- `none`: no usa ningún almacenamiento. El sistema descarta todos los registros, pero aún puede reenviarlos.

La ventaja de los diarios (journals) del sistema almacenados de forma persistente es que los datos históricos están disponibles de inmediato en el inicio. Sin embargo, incluso cuando el diario (journal) se almacene de forma persistente, no todos los datos se conservan para siempre. El diario (journal) tiene un mecanismo de rotación de registro incorporado que se desencadena mensualmente. Además, los diarios (journals) no pueden tener más del 10 % del sistema de archivos en el que están ubicados ni dejar menos del 15 % del sistema de archivos libre. Puede modificar estos valores para el tiempo de ejecución y los diarios (journals) persistentes en el archivo de configuración `/etc/systemd/journald.conf`.

Los límites actuales en cuanto al tamaño del diario (journal) se registran cuando inicia el proceso `systemd-journald`. En el siguiente resultado de comando, se muestran las entradas del diario (journal) que reflejan los límites de tamaño actuales:

```
[user@host ~]$ journalctl | grep -E 'Runtime Journal|System Journal'
Mar 15 04:21:14 localhost systemd-journald[226]: Runtime Journal (/run/log/
journal/4ec03abd2f7b40118b1b357f479b3112) is 8.0M, max 113.3M, 105.3M free.
Mar 15 04:21:19 host.lab.example.com systemd-journald[719]: Runtime Journal (/run/
log/journal/4ec03abd2f7b40118b1b357f479b3112) is 8.0M, max 113.3M, 105.3M free.
Mar 15 04:21:19 host.lab.example.com systemd-journald[719]: System Journal (/run/
log/journal/4ec03abd2f7b40118b1b357f479b3112) is 8.0M, max 4.0G, 4.0G free.
```

**nota**

En el comando `grep` anterior, el símbolo de la barra vertical (`|`) funciona como un operador o. Es decir, el comando `grep` coincide con cualquier línea que contenga la cadena `Runtime Journal` o la cadena `System Journal` de la salida del comando `journalctl`. Este comando captura los límites de tamaño actuales en el almacenamiento volátil del diario (journal) (`Runtime`), así como en el almacenamiento persistente del diario (`System`).

Configuración de diarios (journals) del sistema persistentes

Para configurar el servicio `systemd-journald` y resguardar los diarios (journals) del sistema de forma persistente en el reinicio, ajuste el parámetro `Storage` al valor `persistent` en el archivo `/etc/systemd/journald.conf`. Ejecute el editor de texto de su elección como superusuario para editar el archivo `/etc/systemd/journald.conf`.

```
[Journal]
Storage=persistent
...output omitted...
```

Reinicie el servicio `systemd-journald` para que se apliquen los cambios de configuración.

```
[root@host ~]# systemctl restart systemd-journald
```

Si el servicio `systemd-journald` se reinicia de forma satisfactoria, el servicio crea el directorio `/var/log/journal` que contiene uno o más subdirectorios. Estos subdirectorios tienen caracteres hexadecimales en sus nombres largos y contienen archivos con la extensión `.journal`. Los archivos binarios `.journal` almacenan las entradas del diario (journal) estructuradas e indexadas.

```
[root@host ~]# ls /var/log/journal
4ec03abd2f7b40118b1b357f479b3112
[root@host ~]# ls /var/log/journal/4ec03abd2f7b40118b1b357f479b3112
system.journal user-1000.journal
```

Mientras los diarios (journals) del sistema persisten en el reinicio, el resultado del comando `journalctl` incluyen entradas del inicio actual del sistema así como de los inicios anteriores. Para limitar el resultado a un inicio específico del sistema, use el comando `journalctl` con la opción `-b`. El siguiente comando `journalctl` recupera las entradas del primer inicio del sistema solamente:

```
[root@host ~]# journalctl -b 1
...output omitted...
```

El siguiente comando `journalctl` recupera las entradas limitadas al segundo inicio del sistema:
El argumento es significativo solo si el sistema se ha reiniciado al menos dos veces:

```
[root@host ~]# journalctl -b 2
...output omitted...
```

Puede enumerar los eventos de arranque del sistema que el comando `journalctl` reconoce mediante el uso de la opción `--list-boots`.

```
[root@host ~]# journalctl --list-boots
-6 27de... Wed 2022-04-13 20:04:32 EDT-Wed 2022-04-13 21:09:36 EDT
-5 6a18... Tue 2022-04-26 08:32:22 EDT-Thu 2022-04-28 16:02:33 EDT
-4 e2d7... Thu 2022-04-28 16:02:46 EDT-Fri 2022-05-06 20:59:29 EDT
-3 45c3... Sat 2022-05-07 11:19:47 EDT-Sat 2022-05-07 11:53:32 EDT
-2 dfae... Sat 2022-05-07 13:11:13 EDT-Sat 2022-05-07 13:27:26 EDT
-1 e754... Sat 2022-05-07 13:58:08 EDT-Sat 2022-05-07 14:10:53 EDT
 0 ee2c... Mon 2022-05-09 09:56:45 EDT-Mon 2022-05-09 12:57:21 EDT
```

El siguiente comando `journalctl` recupera las entradas limitadas al inicio del sistema actual:

```
[root@host ~]# journalctl -b
...output omitted...
```



nota

Cuando se depura el bloqueo de un sistema con un diario (journal) persistente, generalmente es necesario limitar la cola del diario al reinicio anterior al bloqueo.

Puede usar el comando `journalctl` con la opción `-b` con un número negativo para indicar cuántos arranques anteriores del sistema se deben incluir en la salida. Por ejemplo, el comando `journalctl -b -1` limita el resultado solo al inicio anterior.



Referencias

Páginas del manual: `systemd-journald.conf(5)`, `systemd-journald(8)`

Para obtener más información, consulte la sección *Troubleshooting Problems Using Log Files* en *Red Hat Enterprise Linux 9 Configuring Basic System Settings Guide* en https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/configuring_basic_system_settings/index#troubleshooting-problems-using-log-files_getting-started-with-system-administration

► Ejercicio Guiado

Resguardo del diario (journal) del sistema

En este ejercicio, configurará el diario (journal) del sistema para preservar sus datos después de un reinicio.

Resultados

- Configurar el diario (journal) del sistema para preservar sus datos después de un reinicio.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start logs-preserve
```

Instrucciones

- 1. Desde la máquina `workstation`, inicie sesión en la máquina `servera` con el usuario `student`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

- 2. Como superusuario, confirme que el directorio `/var/log/journal` no existe. Use el comando `ls` para enumerar el contenido del directorio `/var/log/journal`. Use el comando `sudo` para elevar los privilegios del usuario `student`. Use la contraseña `student` si se le solicita una.

```
[student@servera ~]$ sudo ls /var/log/journal
[sudo] password for student: student
ls: cannot access '/var/log/journal': No such file or directory
```

Debido a que el directorio `/var/log/journal` no existe, el servicio `systemd-journald` no conserva los datos de registro después de un reinicio.

- 3. Configure el servicio `systemd-journald` en la máquina `servera` para resguardar sus diarios (journals) tras un reinicio.

- 3.1. Elimine el comentario de la línea `Storage=auto` en el archivo `/etc/systemd/journald.conf` y ajuste el parámetro `Storage` en el valor `persistent`. Puede usar el comando `sudo vim /etc/systemd/journald.conf` para editar el archivo de configuración. Puede escribir `/Storage=auto` en el modo de comando del editor `vim` para buscar la línea `Storage=auto`.

```
...output omitted...
[Journal]
Storage=persistent
...output omitted...
```

- 3.2. Reinicie el servicio `systemd-journald` para que se apliquen los cambios de configuración.

```
[student@servera ~]$ sudo systemctl restart systemd-journald.service
```

- 4. Verifique que el servicio `systemd-journald` en la máquina `servera` conserve sus diarios (`journals`) para que persistan después de un reinicio.

- 4.1. Reinicie la máquina `servera`.

```
[student@servera ~]$ sudo systemctl reboot
Connection to servera closed by remote host.
Connection to servera closed.
[student@workstation ~]$
```

La conexión SSH finaliza tan pronto como reinicia la máquina `servera`.

- 4.2. Inicie sesión en la máquina `servera`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

- 4.3. Verifique que exista el directorio `/var/log/journal`. El directorio `/var/log/journal` contiene un subdirectorio que tiene un nombre extenso hexadecimal. Puede encontrar los archivos de diario (`journal`) en ese directorio. El nombre del subdirectorio en su sistema será diferente.

```
[student@servera ~]$ sudo ls /var/log/journal
[sudo] password for student: student
63b272eae8d5443ca7aaa5593479b25f
[student@servera ~]$ sudo ls /var/log/journal/63b272eae8d5443ca7aaa5593479b25f
system.journal user-1000.journal
```

- 4.4. Regrese al sistema `workstation` como el usuario `student`.

```
[student@servera ~]$ exit
logout
Connection to servera closed.
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish logs-preserve
```

Esto concluye la sección.

Mantenimiento de la hora correcta

Objetivos

Mantener una sincronización de hora precisa por medio del Protocolo de Tiempo de la Red (NTP) y configurar la zona horaria para garantizar marcas de tiempo correctas para los eventos registrados por el diario (journal) y los registros del sistema.

Administración de relojes y zonas horarias locales

La sincronización de la hora correcta del sistema es fundamental para el análisis del archivo de registro en varios sistemas. Además, algunos servicios pueden requerir sincronización de tiempo para funcionar correctamente. El Protocolo de Tiempo de 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, como el NTP Pool Project. Otra opción es sincronizar con 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 actuales del sistema relacionados con la hora, que incluyen la hora actual, la zona horaria y los parámetros de sincronización de NTP del sistema.

```
[user@host ~]$ timedatectl
          Local time: Wed 2022-03-16 05:53:05 EDT
          Universal time: Wed 2022-03-16 09:53:05 UTC
                RTC time: Wed 2022-03-16 09:53:05
                  Time zone: America/New_York (EDT, -0400)
        System clock synchronized: yes
           NTP service: active
      RTC in local TZ: no
```

Puede enumerar una base de datos de zonas horarias con el comando `timedatectl` con la opción `list-timezones`.

```
[user@host ~]$ timedatectl list-timezones
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
Africa/Asmara
Africa/Bamako
...output omitted...
```

La Autoridad de Números Asignados de Internet (IANA) proporciona una base de datos de zona horaria pública, y el comando `timedatectl` basa los nombres de zona horaria en esa base de datos. Las zonas horarias de la IANA se nombran según el continente u océano; luego, por lo general, aunque no siempre, por 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 `America/Denver`.

capítulo 12 | Analizar y almacenar registros

Algunas localidades dentro de la zona horaria tienen diferentes reglas de horario de verano. Por ejemplo, en los EE. UU., gran parte del estado de Arizona (hora de la zona de montaña de los EE. UU.) no modifica la hora para aprovechar la luz solar y su zona horaria es America/Phoenix.

Use el comando `tzselect` para identificar el nombre correcto de la zona horaria. De manera interactiva, este comando le formula preguntas al usuario sobre la ubicación del sistema y se proporciona el nombre de la zona horaria correcta. No implementa ningún cambio en la configuración de la zona horaria del sistema.

El usuario `root` puede cambiar la configuración del sistema para actualizar la zona horaria actual mediante el comando `timedatectl` con la opción `set-timezone`. Por ejemplo, el siguiente comando `timedatectl` actualiza la zona horaria actual a America/Phoenix.

```
[root@host ~]# timedatectl set-timezone America/Phoenix
[root@host ~]# timedatectl
    Local time: Wed 2022-03-16 03:05:55 MST
    Universal time: Wed 2022-03-16 10:05:55 UTC
          RTC time: Wed 2022-03-16 10:05:55
        Time zone: America/Phoenix (MST, -0700)
System clock synchronized: yes
          NTP service: active
    RTC in local TZ: no
```

**nota**

En caso de que necesite usar el horario universal coordinado (UTC) en un servidor en particular, establezca su zona horaria en UTC. El comando `tzselect` no incluye el nombre de la zona horaria UTC. Use el comando `timedatectl set-timezone UTC` para configurar la zona horaria actual del sistema en UTC.

Use el comando `timedatectl` con la opción `set-time` para cambiar la hora actual del sistema. Puede especificar la hora con el formato "DD-MM-AAAA hh:mm:ss", donde puede omitir la fecha o la hora. Por ejemplo, el siguiente comando `timedatectl` cambia la hora a 09:00:00.

```
[root@host ~]# timedatectl set-time 9:00:00
[root@host ~]# timedatectl
    Local time: Fri 2019-04-05 09:00:27 MST
    Universal time: Fri 2019-04-05 16:00:27 UTC
          RTC time: Fri 2019-04-05 16:00:27
        Time zone: America/Phoenix (MST, -0700)
System clock synchronized: yes
          NTP service: active
    RTC in local TZ: no
```

**nota**

El ejemplo anterior puede fallar con el mensaje de error "Error al establecer la hora: la sincronización automática de la hora está habilitada". En ese caso, primero deshabilite la sincronización automática de la hora antes de configurar manualmente la fecha o la hora, como se explica después de esta nota.

El comando `timedatectl` con la opción `set-ntp` habilita o deshabilita la sincronización de NTP para el ajuste de hora automático. La opción requiere de un argumento `true` o `false` para activarla o desactivarla. Por ejemplo, el siguiente comando `timedatectl` desactiva la sincronización de NTP.

```
[root@host ~]# timedatectl set-ntp false
```



nota

En Red Hat Enterprise Linux 9, el comando `timedatectl set-ntp` ajusta si el servicio NTP `chrony` está habilitado. Otras distribuciones de Linux pueden usar esta configuración para ajustar un servicio NTP o de *Protocolo de Tiempo Simple de Red (SNTP)* diferente.

Habilitar o deshabilitar NTP usando otras utilidades en Red Hat Enterprise Linux, como la aplicación gráfica `GNOME Settings`, también actualiza esta configuración.

Configurar y monitorear el servicio `chrony`

El servicio `chrony` mantiene el *reloj en tiempo real (RTC)*, que suele ser impreciso, según lo programado al sincronizarlo con los servidores NTP configurados. Si no hay conectividad de red disponible, `chrony` calcula la desviación del reloj RTC, que se registra en el valor `driftfile` especificado en el archivo de configuración `/etc/chrony.conf`.

De manera predeterminada, el servicio `chrony` usa servidores de NTP Pool Project para sincronizar la hora y no necesita otra configuración. Es posible que deba cambiar los servidores NTP para una máquina que se ejecuta en una red aislada.

El *estrato* de la fuente de hora de NTP determina su calidad. 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 `stratum 0`. Un servidor NTP conectado en forma directa a dicho reloj es una fuente de hora `stratum 1`, mientras que una máquina que sincroniza la hora a partir de un servidor NTP es una fuente de hora de `stratum 2`.

Existen dos categorías de fuentes de hora, `servidor` y `par`, que puede declarar en el archivo de configuración `/etc/chrony.conf`. La categoría `server` se encuentra un estrato más arriba que el servidor NTP local, y la categoría `peer` está en el mismo estrato. Puede definir varios servidores y pares en el archivo de configuración `chrony`, 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 especificar una serie de opciones para el servidor. Red Hat recomienda usar la opción `iburst` porque, una vez que se inicie el servicio `chrony`, se realizarán cuatro mediciones en un período breve a fin de lograr una sincronización del reloj inicial más precisa. Use el comando `man 5 chrony.conf` para obtener más información acerca de las opciones del archivo de configuración `chrony`.

Como ejemplo, con la siguiente línea `server classroom.example.com iburst` en el archivo de configuración `/etc/chrony.conf`, el servicio `chrony` usa el servidor `classroom.example.com` como fuente de hora NTP.

```
# Use public servers from the pool.ntp.org project.
...output omitted...
server classroom.example.com iburst
...output omitted...
```

Después de orientar el servicio `chrony` hacia la fuente de hora local `classroom.example.com`, deberá reiniciar el servicio.

```
[root@host ~]# systemctl restart chronyd
```

El comando `chronyc sources` actúa como cliente para el servicio `chrony`. Después de configurar la sincronización de NTP, verifique que el sistema local esté usando sin problemas el servidor NTP para sincronizar el reloj del sistema por medio del comando `chronyc sources`. Para obtener un resultado más extenso con explicaciones adicionales, use el comando `chronyc sources -v`.

```
[root@host ~]# chronyc sources -v

-- Source mode '^' = server, '=' = peer, '#' = local clock.
/ .- Source state '*' = current best, '+' = combined, '-' = not combined,
| /           'x' = may be in error, '~' = too variable, '?' = unusable.
||           .- xxxx [ yyyy ] +/- zzzz
||           |     xxxx = adjusted offset,
||           |     yyyy = measured offset,
||           |     zzzz = estimated error.
||           \     |
MS Name/IP address      Stratum Poll Reach LastRx Last sample
=====
^* 172.25.254.254        3      6    17    26 +2957ns[+2244ns] +/-   25ms
```

El carácter de asterisco (*) en el campo S (estado Fuente) indica que el servicio `chrony` usó el servidor `classroom.example.com` como fuente de hora, y el servidor NTP es la máquina que se toma actualmente como referencia para la sincronización.



Referencias

Páginas del manual: `timedatectl(1)`, `tzselect(8)`, `chronyd(8)`, `chrony.conf(5)` y `chronyc(1)`

NTP Pool Project

<http://www.ntppool.org/>

Base de datos de zona horaria

<http://www.iana.org/time-zones>

► Ejercicio Guiado

Mantenimiento de la hora correcta

En este ejercicio, ajusta la zona horaria en un servidor y se asegura de que el reloj de su sistema esté sincronizado con una fuente de hora de NTP.

Resultados

- Cambiar la zona horaria en un servidor.
- Configurar el servidor para sincronizar su hora con una fuente de hora de NTP.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start logs-maintain
```

Instrucciones

- 1. Inicie sesión en la máquina `servera` como el usuario `student`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

- 2. Para esta práctica, imagine que la máquina `servera` se reubica en Haití y necesita actualizar la zona horaria. Eleve los privilegios del usuario `student` mientras ejecuta el comando `timedatectl` para actualizar la zona horaria.

2.1. Seleccione la zona horaria adecuada para Haití.

```
[student@servera ~]$ tzselect
Please identify a location so that time zone rules can be set correctly.
Please select a continent, ocean, "coord", or "TZ".
 1) Africa
 2) Americas
 3) Antarctica
 4) Asia
 5) Atlantic Ocean
 6) Australia
 7) Europe
 8) Indian Ocean
 9) Pacific Ocean
10) coord - I want to use geographical coordinates.
11) TZ - I want to specify the timezone using the Posix TZ format.
```

```
#? 2
Please select a country whose clocks agree with yours.
1) Anguilla    19) Dominican Republic    37) Peru
2) Antigua & Barbuda  20) Ecuador      38) Puerto Rico
3) Argentina   21) El Salvador     39) St Barthelemy
4) Aruba       22) French Guiana   40) St Kitts & Nevis
5) Bahamas     23) Greenland      41) St Lucia
6) Barbados    24) Grenada        42) St Maarten (Dutch)
7) Belize      25) Guadeloupe     43) St Martin (French)
8) Bolivia     26) Guatemala      44) St Pierre & Miquelon
9) Brazil      27) Guyana         45) St Vincent
10) Canada     28) Haiti          46) Suriname
11) Caribbean NL 29) Honduras      47) Trinidad & Tobago
12) Cayman Islands 30) Jamaica      48) Turks & Caicos Is
13) Chile       31) Martinique     49) United States
14) Colombia    32) Mexico         50) Uruguay
15) Costa Rica  33) Montserrat    51) Venezuela
16) Cuba        34) Nicaragua      52) Virgin Islands (UK)
17) Curaçao     35) Panama        53) Virgin Islands (US)
18) Dominica    36) Paraguay
```

#? 28

The following information has been given:

Haiti

Therefore TZ='America/Port-au-Prince' will be used.

Selected time is now: Wed Mar 16 07:10:35 EDT 2022.

Universal Time is now: Wed Mar 16 11:10:35 UTC 2022.

Is the above information OK?

1) Yes

2) No

#? 1

You can make this change permanent for yourself by appending the line

TZ='America/Port-au-Prince'; export TZ

to the file '.profile' in your home directory; then log out and log in again.

Here is that TZ value again, this time on standard output so that you can use the /usr/bin/tzselect command in shell scripts:

America/Port-au-Prince

2.2. Actualice la zona horaria en la máquina servera a America/Port-au-Prince.

```
[student@servera ~]$ sudo timedatectl set-timezone \
America/Port-au-Prince
[sudo] password for student: student
```

2.3. Verifique que haya configurado correctamente la zona horaria en America/Port-au-Prince.

```
[student@servera ~]$ timedatectl
    Local time: Wed 2022-03-16 07:13:25 EDT
    Universal time: Wed 2022-03-16 11:13:25 UTC
        RTC time: Wed 2022-03-16 11:13:24
        Time zone: America/Port-au-Prince (EDT, -0400)
System clock synchronized: no
          NTP service: inactive
    RTC in local TZ: no
```

- 3. Configure el servicio `chronyd` en la máquina `servera` para sincronizar la hora del sistema con el servidor `classroom.example.com` como la fuente de hora de NTP.

- 3.1. Edite el archivo de configuración `/etc/chrony.conf` para especificar el servidor `classroom.example.com` como la fuente de hora de NTP. En la siguiente salida, se muestra la línea de configuración para agregar al archivo de configuración, que incluye la opción `iburst` para acelerar la sincronización de tiempo inicial:

```
...output omitted...
server classroom.example.com iburst
...output omitted...
```

- 3.2. Habilite la sincronización de tiempo en la máquina `servera`. El comando activa el servidor NTP con la configuración modificada en el archivo de configuración `/etc/chrony.conf`. El comando puede activar el servicio `chronyd` o el servicio `ntpd` según lo que esté instalado actualmente en el sistema.

```
[student@servera ~]$ sudo timedatectl set-ntp true
```

- 4. Verifique que los ajustes de configuración `servera` se sincronicen con la fuente de hora de `classroom.example.com` en el entorno del aula.

- 4.1. Verifique que la sincronización de tiempo esté habilitada en la máquina `servera`.



nota

Si en el resultado se muestra que el reloj no está sincronizado, espere dos segundos y vuelva a ejecutar el comando `timedatectl`. La sincronización correcta de los ajustes de hora con la fuente de hora tarda unos segundos.

```
[student@servera ~]$ timedatectl
    Local time: Wed 2022-03-16 07:24:13 EDT
    Universal time: Wed 2022-03-16 11:24:13 UTC
        RTC time: Wed 2022-03-16 11:24:13
        Time zone: America/Port-au-Prince (EDT, -0400)
System clock synchronized: yes
          NTP service: active
    RTC in local TZ: no
```

- 4.2. Verifique que la máquina `servera` esté sincronizando actualmente sus ajustes de hora con la fuente de hora de `classroom.example.com`.

En el resultado se muestra un asterisco (*) en el campo de estado de la fuente (S) para la fuente de hora de NTP `classroom.example.com`. El asterisco indica que la hora del sistema local está sincronizada de forma correcta con la fuente de hora de NTP.

```
[student@servera ~]$ chronyc sources -v

-- Source mode '^' = server, '=' = peer, '#' = local clock.
/ .. Source state '*' = current best, '+' = combined, '-' = not combined,
| /           'x' = may be in error, '~' = too variable, '?' = unusable.
||                                .- xxxx [ yyyy ] +/- zzzz
||      Reachability register (octal) -.          | xxxx = adjusted offset,
||      Log2(Polling interval) --.          |          | yyyy = measured offset,
||                                \          |          | zzzz = estimated error.
||                                |          |
MS Name/IP address      Stratum Poll Reach LastRx Last sample
=====
^* 172.25.254.254          2   6   377   33    +84us[ +248us] +/-   21ms
```

4.3. Regrese al sistema `workstation` como el usuario `student`.

```
[student@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish logs-maintain
```

Esto concluye la sección.

► Trabajo de laboratorio

Analizar y almacenar registros

En este trabajo de laboratorio, cambia la zona horaria en un servidor existente y configura un nuevo archivo de registro para todos los eventos relacionados con fallas de autenticación.

Resultados

- Actualizar la zona horaria en un servidor existente.
- Configurar un nuevo archivo de registro para almacenar todos los mensajes relacionados con fallas de autenticación.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start logs-review
```

Instrucciones

1. Inicie sesión en la máquina `serverb` como el usuario `student`.
2. Suponga que la máquina `serverb` se ha reubicado en Jamaica y, por lo tanto, usted debe actualizar la zona horaria. Verifique que haya configurado correctamente la zona horaria.
3. Visualice todos los eventos de registro registrados en los últimos 30 minutos en la máquina `serverb`.
4. Cree el archivo `/etc/rsyslog.d/auth-errors.conf`. Configure el servicio `rsyslog` para escribir mensajes de autenticación y seguridad en el archivo `/var/log/auth-errors`. Use la utilidad `authpriv` y la prioridad `alert`.

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade logs-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish logs-review
```

Esto concluye la sección.

► Solución

Analizar y almacenar registros

En este trabajo de laboratorio, cambia la zona horaria en un servidor existente y configura un nuevo archivo de registro para todos los eventos relacionados con fallas de autenticación.

Resultados

- Actualizar la zona horaria en un servidor existente.
- Configurar un nuevo archivo de registro para almacenar todos los mensajes relacionados con fallas de autenticación.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start logs-review
```

Instrucciones

1. Inicie sesión en la máquina `serverb` como el usuario `student`.

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
[student@serverb ~]$
```

2. Suponga que la máquina `serverb` se ha reubicado en Jamaica y, por lo tanto, usted debe actualizar la zona horaria. Verifique que haya configurado correctamente la zona horaria.

2.1. Seleccione la zona horaria adecuada para Jamaica.

```
[student@serverb ~]$ tzselect
Please identify a location so that time zone rules can be set correctly.
Please select a continent, ocean, "coord", or "TZ".
1) Africa
2) Americas
3) Antarctica
4) Asia
5) Atlantic Ocean
6) Australia
7) Europe
8) Indian Ocean
9) Pacific Ocean
10) coord - I want to use geographical coordinates.
11) TZ - I want to specify the timezone using the Posix TZ format.
#? 2
```

Please select a country whose clocks agree with yours.

1) Anguilla	19) Dominican Republic	37) Peru
2) Antigua & Barbuda	20) Ecuador	38) Puerto Rico
3) Argentina	21) El Salvador	39) St Barthelemy
4) Aruba	22) French Guiana	40) St Kitts & Nevis
5) Bahamas	23) Greenland	41) St Lucia
6) Barbados	24) Grenada	42) St Maarten (Dutch)
7) Belize	25) Guadeloupe	43) St Martin (French)
8) Bolivia	26) Guatemala	44) St Pierre & Miquelon
9) Brazil	27) Guyana	45) St Vincent
10) Canada	28) Haiti	46) Suriname
11) Caribbean NL	29) Honduras	47) Trinidad & Tobago
12) Cayman Islands	30) Jamaica	48) Turks & Caicos Is
13) Chile	31) Martinique	49) United States
14) Colombia	32) Mexico	50) Uruguay
15) Costa Rica	33) Montserrat	51) Venezuela
16) Cuba	34) Nicaragua	52) Virgin Islands (UK)
17) Curaçao	35) Panama	53) Virgin Islands (US)
18) Dominica	36) Paraguay	

#? 30

The following information has been given:

Jamaica

Therefore TZ='America/Jamaica' will be used.

Selected time is now: Wed Mar 16 07:17:15 EST 2022.

Universal Time is now: Wed Mar 16 12:17:15 UTC 2022.

Is the above information OK?

- 1) Yes
- 2) No

#? 1

You can make this change permanent for yourself by appending the line

TZ='America/Jamaica'; export TZ

to the file '.profile' in your home directory; then log out and log in again.

Here is that TZ value again, this time on standard output so that you can use the /usr/bin/tzselect command in shell scripts:

America/Jamaica

- 2.2. Eleve los privilegios del usuario student para actualizar la zona horaria del servidor serverb a America/Jamaica.

```
[student@serverb ~]$ sudo timedatectl set-timezone America/Jamaica
[sudo] password for student: student
```

- 2.3. Verifique que haya configurado correctamente la zona horaria en America/Jamaica.

```
[student@serverb ~]$ timedatectl
    Local time: Wed 2022-03-16 07:18:40 EST
    Universal time: Wed 2022-03-16 12:18:40 UTC
        RTC time: Wed 2022-03-16 12:18:40
      Time zone: America/Jamaica (EST, -0500)
System clock synchronized: yes
          NTP service: active
    RTC in local TZ: no
```

3. Visualice todos los eventos de registro registrados en los últimos 30 minutos en la máquina serverb.

- 3.1. Determine el período para ver las entradas del diario (journal).

```
[student@serverb ~]$ date
Wed Mar 16 07:19:29 AM EST 2022
[student@serverb ~]$ date -d "-30 minutes"
Wed Mar 16 06:49:38 AM EST 2022
```

- 3.2. Visualice todos los eventos de registro registrados en los últimos 30 minutos en la máquina serverb.

```
[student@serverb ~]$ journalctl --since 06:49:00 --until 07:19:00
...output omitted...
Mar 16 07:10:58 localhost kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB
    WP UC- WT
Mar 16 07:10:58 localhost kernel: found SMP MP-table at [mem
    0x000f5bd0-0x000f5bdf]
Mar 16 07:10:58 localhost kernel: Using GB pages for direct mapping
Mar 16 07:10:58 localhost kernel: RAMDISK: [mem 0x2e0d9000-0x33064fff]
Mar 16 07:10:58 localhost kernel: ACPI: Early table checksum verification disabled
Mar 16 07:10:58 localhost kernel: ACPI: RSDP 0x0000000000F5B90 000014 (v00
    BOCHS )
Mar 16 07:10:58 localhost kernel: ACPI: RSDT 0x000000007FFE12C4 00002C (v01 BOCHS
    BXPCRSDT 00000001 BXPC 00000001)
Mar 16 07:10:58 localhost kernel: ACPI: FACP 0x000000007FFE11D0 000074 (v01 BOCHS
    BXPCFACP 00000001 BXPC 00000001)
Mar 16 07:10:58 localhost kernel: ACPI: DSDT 0x000000007FFDFDC0 001410 (v01 BOCHS
    BXPCDSDT 00000001 BXPC 00000001)
lines 1-50/50 q
[student@serverb ~]$
```

4. Cree el archivo /etc/rsyslog.d/auth-errors.conf. Configure el servicio rsyslog para escribir mensajes de autenticación y seguridad en el archivo /var/log/auth-errors. Use la utilidad authpriv y la prioridad alert.

- 4.1. Cree el archivo /etc/rsyslog.d/auth-errors.conf y especifique el archivo /var/log/auth-errors nuevo como destino para los mensajes de autenticación y seguridad.

```
authpriv.alert  /var/log/auth-errors
```

- 4.2. Reinicie el servicio `rsyslog` para que se apliquen los cambios del archivo de configuración.

```
[student@serverb ~]$ sudo systemctl restart rsyslog
```

- 4.3. Escriba un mensaje de registro de ejemplo en el archivo `/var/log/auth-errors`.

```
[student@serverb ~]$ logger -p authpriv.alert "Logging test authpriv.alert"
```

- 4.4. Verifique que el archivo `/var/log/auth-errors` contenga la entrada de registro con el mensaje `Logging test authpriv.alert`.

```
[student@serverb ~]$ sudo tail /var/log/auth-errors
Mar 16 07:25:12 serverb student[1339]: Logging test authpriv.alert
```

- 4.5. Regrese al sistema `workstation` como el usuario `student`.

```
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@workstation ~]$
```

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade logs-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish logs-review
```

Esto concluye la sección.

Resumen

- Los servicios `systemd-journald` y `rsyslog` capturan y escriben mensajes de registro en los archivos correspondientes.
- El directorio `/var/log` contiene archivos de registro.
- La rotación periódica de los archivos de registro evita que llenen el espacio del sistema de archivos.
- Los diarios (journals) de `systemd` son temporales y no se guardan tras un reinicio.
- El servicio `chrony` ayuda a sincronizar los ajustes de hora con una fuente de hora.
- Puede actualizar la zona horaria del servidor en función de su ubicación.

capítulo 13

Administración de redes

Meta

Configurar las interfaces de red y la configuración en servidores Red Hat Enterprise Linux.

Objetivos

- Probar e inspeccionar la configuración de red actual con las utilidades de la línea de comando.
- Administrar los parámetros de configuración de red con el comando nmcli.
- Modificar la configuración de la red mediante la edición de los archivos de configuración.
- Configurar el nombre de host estático del servidor y su resolución de nombre, y probar los resultados.

Secciones

- Validación de la configuración de red (y ejercicio guiado)
- Configuración de redes desde la línea de comandos (y ejercicio guiado)
- Edición de los archivos de configuración de red (y ejercicio guiado)
- Configuración de nombres de host y resolución de nombre (y ejercicio guiado)

Trabajo de laboratorio

- Administración de redes

Validación de la configuración de red

Objetivos

Probar e inspeccionar la configuración de red actual con las utilidades de la línea de comando.

Recopilación de la información de interfaz de red

El comando `ip link` enumera todas las interfaces de red disponibles en su sistema. En el siguiente ejemplo, el servidor tiene tres interfaces de red: `lo`, que es el dispositivo de bucle invertido que está conectado al propio servidor, y dos interfaces Ethernet, `ens3` y `ens4`.

```
[user@host ~]$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
    group default qlen 1000
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT
    group default qlen 1000
        link/ether 52:54:00:00:00:0a brd ff:ff:ff:ff:ff:ff
3: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT
    group default qlen 1000
        link/ether 52:54:00:00:00:1e brd ff:ff:ff:ff:ff:ff
```

Para configurar una interfaz de red correctamente, debe saber qué interfaz está conectada a qué red. En muchos casos, puede obtener la dirección MAC de la interfaz conectada a cada red, ya sea porque está impresa físicamente en la tarjeta o el servidor, o porque es una máquina virtual y usted sabe cómo está configurada. La dirección MAC del dispositivo aparece después de `link/ether` para cada interfaz. Así que ya sabes que la tarjeta de red con la dirección MAC `52:54:00:00:00:0a` es la interfaz de red `ens3`.

Visualización de las direcciones IP

Use el comando `ip` para ver la información del dispositivo y de la dirección. Una sola interfaz de red puede tener varias direcciones IPv4 o IPv6.

```
[user@host ~]$ ip addr show ens3
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000①
    link/ether 52:54:00:00:00:0b brd ff:ff:ff:ff:ff:ff②
        inet 192.0.2.2/24 brd 192.0.2.255 scope global ens3③
            valid_lft forever preferred_lft forever
        inet6 2001:db8:0:1:5054:ff:fe00:b/64 scope global④
            valid_lft forever preferred_lft forever
        inet6 fe80::5054:ff:fe00:b/64 scope link⑤
            valid_lft forever preferred_lft forever
```

① Una interfaz activa está UP.

② La cadena `link/ether` especifica la dirección de hardware (MAC) del dispositivo.

- ③ La cadena `inet` muestra una dirección IPv4, la longitud del prefijo de red y el alcance.
- ④ La cadena `inet6` muestra una dirección IPv6, la longitud del prefijo de red y el alcance. Esta dirección es de alcance *global* y se usa con normalidad.
- ⑤ Esta cadena `inet6` muestra que la interfaz tiene una dirección IPv6 del alcance de *vínculo* que solo puede usarse para la comunicación en el vínculo de Ethernet local.

Visualización de estadísticas de rendimiento

El comando `ip` también puede mostrar estadísticas sobre el rendimiento de la red. Los contadores para cada interfaz de red pueden identificar la presencia de problemas de red. Los contadores registran estadísticas para cosas como la cantidad de paquetes recibidos (RX) y transmitidos (TX), errores de paquetes y paquetes omitidos.

```
[user@host ~]$ ip -s link show ens3
2: ens3: <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
```

Comprobación de la conectividad entre hosts

El comando `ping` prueba la conectividad. El comando continúa ejecutándose hasta que se presione `Ctrl+C`, a menos que se indiquen otras opciones para limitar la cantidad de paquetes enviados.

```
[user@host ~]$ ping -c3 192.0.2.254
PING 192.0.2.1 (192.0.2.254) 56(84) bytes of data.
64 bytes from 192.0.2.254: icmp_seq=1 ttl=64 time=4.33 ms
64 bytes from 192.0.2.254: icmp_seq=2 ttl=64 time=3.48 ms
64 bytes from 192.0.2.254: icmp_seq=3 ttl=64 time=6.83 ms

--- 192.0.2.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 3.485/4.885/6.837/1.424 ms
```

El comando `ping6` es la versión de IPv6 del comando `ping` en Red Hat Enterprise Linux. La diferencia entre estos comandos es que el comando `ping6` se comunica a través de IPv6 y toma direcciones IPv6.

```
[user@host ~]$ ping6 2001:db8:0:1::1
PING 2001:db8:0:1::1(2001:db8:0:1::1) 56 data bytes
64 bytes from 2001:db8:0:1::1: icmp_seq=1 ttl=64 time=18.4 ms
64 bytes from 2001:db8:0:1::1: icmp_seq=2 ttl=64 time=0.178 ms
64 bytes from 2001:db8:0:1::1: icmp_seq=3 ttl=64 time=0.180 ms
^C
--- 2001:db8:0:1::1 ping statistics ---
```

```
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.178/6.272/18.458/8.616 ms
[user@host ~]$
```

Cuando hace ping a las direcciones de enlace-local y al grupo multidifusión (multicast) de todos los nodos de enlace-local (`ff02::1`), la interfaz de red que se debe usar debe especificarse explícitamente con un identificador de zona de alcance (como `ff02::1%ens3`). Si se omite esta interfaz de red, se muestra el error de conexión: *argumento no válido*.

Puede usar el comando `ping6 ff02::1` para buscar otros nodos IPv6 en la red local.

```
[user@host ~]$ ping6 ff02::1%ens4
PING ff02::1%ens4(ff02::1) 56 data bytes
64 bytes from fe80::78cf:ffff:fed2:f97b: icmp_seq=1 ttl=64 time=22.7 ms
64 bytes from fe80::f482:dbff:fe25:6a9f: icmp_seq=1 ttl=64 time=30.1 ms (DUP!)
64 bytes from fe80::78cf:ffff:fed2:f97b: icmp_seq=2 ttl=64 time=0.183 ms
64 bytes from fe80::f482:dbff:fe25:6a9f: icmp_seq=2 ttl=64 time=0.231 ms (DUP!)
^C
--- ff02::1%ens4 ping statistics ---
2 packets transmitted, 2 received, +2 duplicates, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.183/13.320/30.158/13.374 ms
[user@host ~]$
[user@host ~]$ ping6 -c 1 fe80::f482:dbff:fe25:6a9f%ens4
PING fe80::f482:dbff:fe25:6a9f%ens4(fe80::f482:dbff:fe25:6a9f) 56 data bytes
64 bytes from fe80::f482:dbff:fe25:6a9f: icmp_seq=1 ttl=64 time=22.9 ms

--- fe80::f482:dbff:fe25:6a9f%ens4 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 22.903/22.903/22.903/0.000 ms
```

Las direcciones de enlace-local de IPv6 pueden ser usadas por otros hosts en el mismo vínculo, al igual que las direcciones normales.

```
[user@host ~]$ ssh fe80::f482:dbff:fe25:6a9f%ens4
user@fe80::f482:dbff:fe25:6a9f%ens4's password:
Last login: Thu Jun  5 15:20:10 2014 from host.example.com
[user@server ~]$
```

Solucionar problemas del enrutador

El enrutamiento de la red es complejo y, a veces, el tráfico no se comporta como se espera. Puede usar diferentes herramientas para diagnosticar problemas del enrutador.

Describir la tabla de enrutamiento

Use el comando `ip` con la opción `route` para mostrar información de enrutamiento.

```
[user@host ~]$ ip route
default via 192.0.2.254 dev ens3 proto static metric 1024
192.0.2.0/24 dev ens3 proto kernel scope link src 192.0.2.2
10.0.0.0/8 dev ens4 proto kernel scope link src 10.0.0.11
```

Todos los paquetes que estén destinados para la red 10.0.0.0/8 se envían directamente al destino mediante el dispositivo ens4. Todos los paquetes que estén destinados para la red 192.0.2.0/24 se envían directamente al destino mediante el dispositivo ens3. Todos los demás paquetes se envían al enrutador predeterminado que está ubicado en 192.0.2.254, y también mediante el dispositivo ens3.

Use el comando `ip` con la opción `-6` para mostrar la tabla de enrutamiento de IPv6.

```
[user@host ~]$ ip -6 route
unreachable ::/96 dev lo metric 1024 error -101
unreachable ::ffff:0.0.0.0/96 dev lo metric 1024 error -101
2001:db8:0:1::/64 dev ens3 proto kernel metric 256
unreachable 2002:a00::/24 dev lo metric 1024 error -101
unreachable 2002:7f00::/24 dev lo metric 1024 error -101
unreachable 2002:a9fe::/32 dev lo metric 1024 error -101
unreachable 2002:ac10::/28 dev lo metric 1024 error -101
unreachable 2002:c0a8::/32 dev lo metric 1024 error -101
unreachable 2002:e000::/19 dev lo metric 1024 error -101
unreachable 3ffe:ffff::/32 dev lo metric 1024 error -101
fe80::/64 dev ens3 proto kernel metric 256
default via 2001:db8:0:1::ffff dev ens3 proto static metric 1024
```

1. La red 2001:db8:0:1::/64 usa la interfaz ens3 (que supuestamente tiene una dirección en esa red).
2. La red fe80::/64 usa la interfaz ens3 para la dirección de enlace-local. En un sistema con múltiples interfaces, hay una ruta a la red fe80::/64 en cada interfaz para cada dirección de enlace-local.
3. La ruta predeterminada a todas las redes en Internet IPv6 (la red ::/0) usa el enrutador en la red 2001:db8:0:1::ffff y es accesible con el dispositivo ens3.

Rastreo de rutas de tráfico

Para rastrear la ruta que toma el tráfico de la red para llegar a un host remoto a través de múltiples enrutadores, use el comando `traceroute` o `tracepath`. Estos comandos pueden identificar si hay un problema con uno de sus enrutadores o con uno intermedio. Ambos comandos usan paquetes de UDP para realizar el seguimiento de una ruta de forma predeterminada; 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). En general, el comando `traceroute` no está instalado de forma predeterminada.

```
[user@host ~]$ tracepath access.redhat.com
...output omitted...
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.atlngamq46w-bcr00.tbone.rr.com 107.286ms asymm 12
...output omitted...
```

Cada línea del resultado del comando `tracepath` representa un router o hop por donde pasa el paquete entre el origen y el destino final. El comando proporciona información adicional para

cada hop según esté disponible, que incluye la sincronización en ambos sentidos (RTT) y cualquier cambio en el tamaño de la unidad de transmisión máxima (MTU). La indicación asymm significa que el tráfico llegó a ese enrutador regresó de ese enrutador usando diferentes rutas (asimétricas). Estos enrutadores aquí son para el tráfico saliente, no para el tráfico de retorno.

Los comandos `tracepath6` y `traceroute -6` son los comandos de IPv6 equivalentes a los comandos `tracepath` y `traceroute`.

```
[user@host ~]$ tracepath6 2001:db8:0:2::451
 1?: [LOCALHOST]          0.091ms pmtu 1500
 1: 2001:db8:0:1::ba    0.214ms
 2: 2001:db8:0:1::1     0.512ms
 3: 2001:db8:0:2::451   0.559ms reached
Resume: pmtu 1500 hops 3 back 3
```

Solución de problemas en puertos y servicios

Los servicios TCP usan sockets como extremos (endpoints) para la comunicación y se componen de una dirección IP, protocolo y número de puerto. En general, los servicios están atentos a los puertos estándares 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` reemplaza la herramienta anterior `netstat`, que es parte del paquete `net-tools`, que algunos administradores de sistemas pueden conocer más, pero que no siempre está instalada.

```
[user@host ~]$ ss -ta
State      Recv-Q Send-Q      Local Address:Port          Peer Address:Port
LISTEN      0      128          *:sunrpc                  *:*
LISTEN      0      128          *:ssh                     *:*①
LISTEN      0      100          127.0.0.1:smtp            :②
LISTEN      0      128          *:36889                  *:*
ESTAB       0      0            172.25.250.10:ssh        172.25.254.254:59392③
LISTEN      0      128          :::sunrpc                 :::*
LISTEN      0      128          :::ssh                    ::*:*④
LISTEN      0      100          ::1:smtp                  ::*:*⑤
LISTEN      0      128          :::34946                  :::*
```

- ① ***:ssh**: Puerto usado para SSH está atento a todas las direcciones IPv4. El carácter de asterisco (*) se usa para indicar *todos* cuando se hace referencia a los puertos o las direcciones IPv4.
- ② **127.0.0.1:smtp**: El puerto usado para SMTP escucha la interfaz de circuito de retorno de la IPv4 127.0.0.1.
- ③ **172.25.250.10:ssh**: La conexión SSH establecida está en la interfaz 172.25.250.10 y se origina de un sistema con una dirección de 172.25.254.254.
- ④ **:::ssh**: Puerto usado para SSH está atento a todas las direcciones IPv6. La sintaxis de dos puntos (:) representa todas las interfaces IPv6.
- ⑤ **::1:smtp**: El puerto usado para SMTP escucha la interfaz de circuito de retorno ::1 IPv6.

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 (los que escucha y los establecidos).
-p	Muestra el proceso de usar los sockets.
-A inet	Muestra las conexiones activas (pero no los sockets que se escuchan) para la familia de direcciones <code>inet</code> . Es decir, ignora los sockets de dominio UNIX local. Para el comando <code>ss</code> , se muestran las conexiones IPv4 e IPv6. Para el comando <code>netstat</code> , se muestran solo las conexiones IPv4. (El comando <code>netstat -A inet6</code> mostrará las conexiones IPv6 y el comando <code>netstat -46</code> mostrará IPv4 e IPv6 al mismo tiempo).



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)`.

Para obtener más información, consulte la *Configuring and Managing Networking Guide* en

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/configuring_and_managing_networking/index

► Ejercicio Guiado

Validación de la configuración de red

En este ejercicio, revisa la configuración de red de uno de sus servidores.

Resultados

- Identificar las interfaces de la red actual y las direcciones básicas de la red.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start net-validate
```

Instrucciones

- 1. Use el comando `ssh` para iniciar sesión en `servera` con el usuario `student`. Los sistemas están configurados para usar claves SSH para la autenticación y acceso sin contraseña para `servera`.

```
[student@workstation ~]$ ssh student@servera  
...output omitted...  
[student@servera ~]$
```

- 2. Localice el nombre de la interfaz de red asociado con la dirección Ethernet `52:54:00:00:fa:0a`. Registre o recuerde este nombre y utilícelo para reemplazar el marcador de posición `enX` en los comandos subsiguientes.



Importante

Los nombres de la interfaz de red están determinados por su tipo de bus y el orden de detección de los dispositivos durante el arranque. Los nombres de la interfaz de red variarán según la plataforma del curso y el hardware en uso.

En su sistema, localice el nombre de la interfaz (como `ens06` o `en1p2`) asociado a la dirección Ethernet `52:54:00:00:fa:0a`. Use este nombre de interfaz para reemplazar el marcador de posición `enX` que se usa a lo largo de este ejercicio.

```
[student@servera ~]$ ip link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    qlen 1000
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enX: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
    default qlen 1000
        link/ether 52:54:00:00:fa:0a brd ff:ff:ff:ff:ff:ff
```

- 3. Visualice la dirección IP y la máscara de red actuales de todas las interfaces.

```
[student@servera ~]$ ip -br addr
lo          UP      127.0.0.1/8 ::1/128
enX:        UP      172.25.250.10/24 fe80::3059:5462:198:58b2/64
```

- 4. Visualice las estadísticas correspondientes a la interfaz enX.

```
[student@servera ~]$ ip -s link show enX
2: enX: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode
    DEFAULT group default qlen 1000
        link/ether 52:54:00:00:fa:0a brd ff:ff:ff:ff:ff:ff
        RX: bytes   packets   errors   dropped overrun mcast
            89014225    168251      0       154418      0       0
        TX: bytes   packets   errors   dropped carrier collsns
            608808     6090      0       0       0       0
```

- 5. Visualice la información de enrutamiento.

```
[student@servera ~]$ ip route
default via 172.25.250.254 dev enX proto static metric 100
172.25.250.0/24 dev enX proto kernel scope link src 172.25.250.10 metric 100
```

- 6. Verifique que se pueda acceder al enrutador.

```
[student@servera ~]$ ping -c3 172.25.250.254
PING 172.25.250.254 (172.25.250.254) 56(84) bytes of data.
64 bytes from 172.25.250.254: icmp_seq=1 ttl=64 time=0.196 ms
64 bytes from 172.25.250.254: icmp_seq=2 ttl=64 time=0.436 ms
64 bytes from 172.25.250.254: icmp_seq=3 ttl=64 time=0.361 ms

--- 172.25.250.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 49ms
rtt min/avg/max/mdev = 0.196/0.331/0.436/0.100 ms
```

- 7. Visualice todos los saltos entre el sistema local y classroom.example.com.

```
[student@servera ~]$ tracepath classroom.example.com
 1?: [LOCALHOST]                                pmtu 1500
 1:  bastion.lab.example.com                   0.337ms
 1:  bastion.lab.example.com                   0.122ms
 2:  172.25.254.254                           0.602ms reached
Resume: pmtu 1500 hops 2 back 2
```

- 8. Visualice los sockets TCP de escucha en el sistema local.

```
[student@servera ~]$ ss -lt
State      Recv-Q Send-Q      Local Address:Port      Peer Address:Port
LISTEN      0      128          0.0.0.0:sunrpc        0.0.0.0:*
LISTEN      0      128          0.0.0.0:ssh           0.0.0.0:*
LISTEN      0      128          [:]:sunrpc          [:]:*
LISTEN      0      128          [:]:ssh             [:]:*
```

- 9. Regrese al sistema workstation como el usuario student.

```
[student@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$
```

Finalizar

En la máquina **workstation**, cambie al directorio de inicio de usuario **student** y use el comando **lab** para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish net-validate
```

Esto concluye la sección.

Configuración de redes desde la línea de comandos

Objetivos

Administrar los parámetros de configuración de red con el comando `nmcli`.

Describir el servicio NetworkManager

El servicio NetworkManager monitorea y administra la configuración de red de un sistema. En el entorno gráfico GNOME, un subprograma del área de notificación muestra la configuración de red y la información de estado que se recibe del daemon NetworkManager. Puede interactuar con el servicio NetworkManager a través de la línea de comandos o con herramientas gráficas. Los archivos de configuración de servicio están almacenados en el directorio `/etc/NetworkManager/system-connections/`.

El servicio NetworkManager administra de manera dinámica *dispositivos* y *conexiones* de red. Un *dispositivo* es una interfaz de red física o virtual que proporciona tráfico de red. Una *conexión* es un conjunto de ajustes de configuración relacionados para un solo dispositivo de red. Una conexión también se conoce como *perfil de red*. Cada conexión debe tener un nombre o ID único, que puede coincidir con el nombre del dispositivo que configura.

Un solo dispositivo puede tener varias configuraciones de conexión y cambiar entre ellas, pero solo una conexión puede estar activa por dispositivo. Por ejemplo, un dispositivo inalámbrico de computadora portátil puede configurar una dirección IP fija para su uso en un sitio de trabajo seguro en una conexión, pero puede configurar una segunda conexión con una dirección automatizada y una red privada virtual (VPN) para acceder a la misma red de la empresa desde casa.



Importante

A partir de Red Hat Enterprise Linux 8, los archivos de configuración de formato `ifcfg` y el directorio `/etc/sysconfig/network-scripts/` están obsoletos. NetworkManager ahora usa un formato de archivo de clave de estilo INI, que es una estructura de par de clave-valor para organizar las propiedades. NetworkManager almacena perfiles de red en el directorio `/etc/NetworkManager/system-connections/`. Para compatibilidad con versiones anteriores, las conexiones de formato `ifcfg` en el directorio `/etc/sysconfig/network-scripts/` aún se reconocen y cargan.

Visualización de información de redes

Use la utilidad `nmcli` para crear y editar archivos de conexión desde la línea de comandos. El comando `nmcli device status` muestra el estado de todos los dispositivos de red:

```
[user@host ~]$ nmcli dev status
DEVICE  TYPE      STATE      CONNECTION
eno1    ethernet  connected  eno1
ens3    ethernet  connected  static-ens3
eno2    ethernet  disconnected  --
lo     loopback  unmanaged  --
```

**nota**

Puede abreviar `nmcli` objetos y acciones. Por ejemplo, puede abreviar `nmcli device disconnect` como `nmcli dev dis` y `nmcli connection modify` como `nmcli con mod`. La abreviatura puede ser tan corta como una sola letra, pero debe usar suficientes caracteres para identificar de manera única el objeto que se debe administrar.

El comando `nmcli connection show` muestra una lista de todas las conexiones. Use la opción `--active` para enumerar solo las conexiones activas.

```
[user@host ~]$ nmcli con show
NAME      UUID                                  TYPE      DEVICE
eno2      ff9f7d69-db83-4fed-9f32-939f8b5f81cd 802-3-ethernet  --
static-ens3 72ca57a2-f780-40da-b146-99f71c431e2b 802-3-ethernet  ens3
eno1      87b53c56-1f5d-4a29-a869-8a7bdaf56dfa 802-3-ethernet  eno1
[user@host ~]$ nmcli con show --active
NAME      UUID                                  TYPE      DEVICE
static-ens3 72ca57a2-f780-40da-b146-99f71c431e2b 802-3-ethernet  ens3
eno1      87b53c56-1f5d-4a29-a869-8a7bdaf56dfa 802-3-ethernet  eno1
```

Adición de una conexión de red

El comando `nmcli connection add` se usa para agregar conexiones de red.

El siguiente ejemplo agrega una conexión para la interfaz `eno2` denominada `eno2`. La información de red para la conexión usa un servicio DHCP y hace que el dispositivo se conecte automáticamente al inicio. El sistema también obtiene configuraciones de red IPv6 al escuchar los anuncios del enrutador en el vínculo local. El nombre del archivo de configuración contiene el valor del parámetro `nmcli` del comando `con-name`, que es `eno2`. El valor del parámetro `con-name` se guarda en el archivo `/etc/NetworkManager/system-connections/eno2.nmconnection`.

```
[root@host ~]# nmcli con add con-name eno2 \
type ethernet iface eno2
Connection 'eno2' (8159b66b-3c36-402f-aa4c-2ea933c7a5ce) successfully added
```

El siguiente ejemplo crea la conexión `eno3` para el dispositivo `eno3` con una configuración de red IPv4 estática. Este comando configura la dirección IP `192.168.0.5` con un prefijo de red de `/24` y una puerta de enlace de red de `192.168.0.254`. El comando `nmcli connection add` falla si el nombre de conexión que intenta agregar existe.

```
[root@host ~]# nmcli con add con-name eno3 type ethernet iface eno3 \
ipv4.addresses 192.168.0.5/24 ipv4.gateway 192.168.0.254
```

El siguiente ejemplo crea la conexión eno4 para el dispositivo eno4 con direcciones IPv6 e IPv4 estáticas. Este comando configura la dirección IPv6 2001:db8:0:1::c000:207 con el prefijo de red /64 y la dirección 2001:db8:0:1::1 como puerta de enlace predeterminada. Este comando también configura la dirección IPv4 192.0.2.7 con el prefijo de red /24 y la dirección 192.0.2.1 como puerta de enlace predeterminada.

```
[root@host ~]# nmcli con add con-name eno4 type ethernet ifname eno4 \
    ipv6.addresses 2001:db8:0:1::c000:207/64 ipv6.gateway 2001:db8:0:1::1 \
    ipv4.addresses 192.0.2.7/24 ipv4.gateway 192.0.2.1
```

Administración de las conexiones de red

El comando `nmcli connection up` activa una conexión de red en el dispositivo al que está unido. La activación de una conexión de red requiere el nombre de la conexión, no el nombre del dispositivo.

```
[user@host ~]$ nmcli con show
NAME           UUID                                  TYPE      DEVICE
static-ens3    72ca57a2-f780-40da-b146-99f71c431e2b  802-3-ethernet  --
static-ens5    87b53c56-1f5d-4a29-a869-8a7bdaf56dfa  802-3-ethernet  --
[root@host ~]# nmcli con up static-ens3
Connection successfully activated (D-Bus active path: /org/freedesktop/
NetworkManager/ActiveConnection/2)
```

El comando `nmcli device disconnect` desconecta el dispositivo de red y cierra la conexión.

```
[root@host ~]# nmcli dev disconnect ens3
```



Importante

Use `nmcli device disconnect` para detener el tráfico en una interfaz de red y desactivar la conexión.

Debido a que la mayoría de las conexiones habilitan el parámetro `autoconnect`, el comando `nmcli connection down` no es efectivo para detener el tráfico. Si bien la conexión se desactiva, la conexión automática reactiva inmediatamente la conexión si el dispositivo está activo y disponible. La conexión automática es un comportamiento deseado porque mantiene las conexiones a través de cortes de red temporales.

Al desconectar el dispositivo en la conexión, se fuerza la desconexión de la conexión hasta que el dispositivo se vuelva a conectar.

Actualización de la configuración de conexión de red

Las conexiones de servicio NetworkManager tienen dos tipos de parámetros. Hay propiedades de conexión estáticas, configuradas por el administrador y almacenadas en los archivos de configuración en `/etc/NetworkManager/system-connections/*.nmconnection`. Las propiedades de conexión dinámica se solicitan desde un servidor DHCP y no se almacenan de forma persistente.

Para enumerar la configuración actual de una conexión, use el comando `nmcli connection show`. Las configuraciones en minúsculas son propiedades estáticas que el administrador

puede cambiar. Las configuraciones en mayúscula son configuraciones activas que se usan provisoriamente para esta instancia de la conexión.

```
[root@host ~]# nmcli con show static-ens3
connection.id:                      static-ens3
connection.uuid:                     87b53c56-1f5d-4a29-a869-8a7bdaf56dfa
connection.interface-name:           --
connection.type:                     802-3-ethernet
connection.autoconnect:              yes
connection.timestamp:                1401803453
connection.read-only:                no
connection.permissions:              --
connection.zone:                     --
connection.master:                   --
connection.slave-type:               --
connection.secondaries:              --
connection.gateway-ping-timeout:    0
802-3-ethernet.port:                --
802-3-ethernet.speed:               0
802-3-ethernet.duplex:              --
802-3-ethernet.auto-negotiate:     yes
802-3-ethernet.mac-address:         CA:9D:E9:2A:CE:F0
802-3-ethernet.cloned-mac-address: --
802-3-ethernet.mac-address-blacklist: --
802-3-ethernet.mtu:                 auto
802-3-ethernet.s390-subchannels:    --
802-3-ethernet.s390-nettype:        --
802-3-ethernet.s390-options:       --
ipv4.method:                        manual
ipv4.dns:                           192.168.0.254
ipv4.dns-search:                    example.com
ipv4.addresses:                     { ip = 192.168.0.2/24,
                                         gw = 192.168.0.254 }
ipv4.routes:                         --
ipv4.ignore-auto-routes:            no
ipv4.ignore-auto-dns:               no
ipv4.dhcp-client-id:                --
ipv4.dhcp-send-hostname:            yes
ipv4.dhcp-hostname:                 --
ipv4.never-default:                 no
ipv4.may-fail:                      yes
ipv6.method:                        manual
ipv6.dns:                           2001:4860:4860::8888
ipv6.dns-search:                    example.com
ipv6.addresses:                     { ip = 2001:db8:0:1::7/64,
                                         gw = 2001:db8:0:1::1 }
ipv6.routes:                         --
ipv6.ignore-auto-routes:            no
ipv6.ignore-auto-dns:               no
ipv6.never-default:                 no
ipv6.may-fail:                      yes
ipv6.ip6-privacy:                  -1 (unknown)
ipv6.dhcp-hostname:                 --
...output omitted...
```

Use el comando `nmcli connection modify` para actualizar la configuración de conexión. Estos cambios se guardan en el archivo `/etc/NetworkManager/system-connections/name.nmconnection`. Consulte la página del manual `nm-settings(5)` para conocer las configuraciones disponibles.

Use el siguiente comando para actualizar la conexión `static-ens3` para establecer la dirección IPv4 `192.0.2.2/24` y la puerta de enlace predeterminada `192.0.2.254`. Use el parámetro `nmcli` comando `connection.autoconnect` para habilitar o deshabilitar automáticamente la conexión en el arranque del sistema.

```
[root@host ~]# nmcli con mod static-ens3 ipv4.addresses 192.0.2.2/24 \
    ipv4.gateway 192.0.2.254 connection.autoconnect yes
```

Use el siguiente comando para actualizar la conexión `static-ens3` para establecer la dirección IPv6 `2001:db8:0:1::a00:1/64` y la puerta de enlace predeterminada `2001:db8:0:1::1`.

```
[root@host ~]# nmcli con mod static-ens3 ipv6.addresses 2001:db8:0:1::a00:1/64 \
    ipv6.gateway 2001:db8:0:1::1
```



Importante

Para cambiar la configuración de una conexión DHCP para que sea estática, actualice la configuración de `ipv4.method` de `auto` o `dhcp` a `manual`. Para una conexión IPv6, actualice la configuración `ipv6.method`. Si el método no se configura correctamente, la conexión puede bloquearse o estar incompleta cuando se activa, o puede obtener una dirección de DHCP o SLAAC además de la dirección estática configurada.

Algunas configuraciones pueden tener varios valores. Es posible agregar un valor específico a la lista o eliminarlo de la configuración de la conexión al agregar un símbolo más (+) o un símbolo menos (-) al comienzo del nombre de la configuración. Si no se incluye un signo más o menos, el valor especificado reemplaza la lista actual de la configuración. El siguiente ejemplo agrega el servidor DNS `2.2.2.2` a la conexión `static-ens3`.

```
[root@host ~]# nmcli con mod static-ens3 +ipv4.dns 2.2.2.2
```

También puede modificar los perfiles de red editando el archivo de configuración de la conexión en `/etc/NetworkManager/system-connections/`. Mientras que los comandos `nmcli` se comunican directamente con `NetworkManager` para implementar modificaciones inmediatamente, las ediciones del archivo de conexión no se implementan hasta que se solicita a `NetworkManager` que vuelva a cargar el archivo de configuración. Con la edición manual, puede crear configuraciones complejas en pasos y, luego, cargar la configuración final cuando esté lista. El siguiente ejemplo carga todos los perfiles de conexión.

```
[root@host ~]# nmcli con reload
```

El siguiente ejemplo carga solo el perfil de conexión `eno2` en `/etc/NetworkManager/system-connections/eno2.nmconnection`.

```
[root@host ~]# nmcli con reload eno2
```

Eliminación de una conexión de red

El comando `nmcli connection delete` elimina una conexión del sistema. Este comando desconecta el dispositivo y elimina el archivo de configuración de la conexión.

```
[root@host ~]# nmcli con del static-ens3
```

Permisos para modificar la configuración de NetworkManager

El usuario `root` puede usar el comando `nmcli` para revisar la configuración de la red.

Los usuarios sin privilegios que han iniciado sesión en la consola física o virtual también pueden realizar la mayoría de los cambios de configuración de red. Si hay una persona en la consola del sistema, es probable que el sistema se esté usando como una estación de trabajo o una computadora portátil donde el usuario necesita configurar, activar y desactivar las conexiones. Los usuarios sin privilegios que inician sesión con `ssh` deben cambiar al usuario `root` para cambiar la configuración de red.

Use el comando `nmcli general permissions` para ver sus permisos actuales. El siguiente ejemplo enumera los permisos NetworkManager del usuario `root`.

```
[root@host ~]# nmcli gen permissions
PERMISSION                                     VALUE
org.freedesktop.NetworkManager.checkpoint-rollback   yes
org.freedesktop.NetworkManager.enable-disable-connectivity-check  yes
org.freedesktop.NetworkManager.enable-disable-network    yes
org.freedesktop.NetworkManager.enable-disable-statistics yes
org.freedesktop.NetworkManager.enable-disable-wifi      yes
org.freedesktop.NetworkManager.enable-disable-wimax    yes
org.freedesktop.NetworkManager.enable-disable-wwan    yes
org.freedesktop.NetworkManager.network-control        yes
org.freedesktop.NetworkManager.reload                yes
org.freedesktop.NetworkManager.settings.modify.global-dns yes
org.freedesktop.NetworkManager.settings.modify.hostname yes
org.freedesktop.NetworkManager.settings.modify.own     yes
org.freedesktop.NetworkManager.settings.modify.system  yes
org.freedesktop.NetworkManager.sleep-wake            yes
org.freedesktop.NetworkManager.wifi.scan             yes
org.freedesktop.NetworkManager.wifi.share.open       yes
org.freedesktop.NetworkManager.wifi.share.protected  yes
```

El siguiente ejemplo enumera los permisos del usuario NetworkManager.

```
[user@host ~]$ nmcli gen permissions
PERMISSION                                     VALUE
org.freedesktop.NetworkManager.checkpoint-rollback auth
org.freedesktop.NetworkManager.enable-disable-connectivity-check no
org.freedesktop.NetworkManager.enable-disable-network  no
org.freedesktop.NetworkManager.enable-disable-statistics no
org.freedesktop.NetworkManager.enable-disable-wifi     no
org.freedesktop.NetworkManager.enable-disable-wimax    no
org.freedesktop.NetworkManager.enable-disable-wwan    no
org.freedesktop.NetworkManager.network-control        auth
org.freedesktop.NetworkManager.reload                auth
```

```

org.freedesktop.NetworkManager.settings.modify.global-dns      auth
org.freedesktop.NetworkManager.settings.modify.hostname       auth
org.freedesktop.NetworkManager.settings.modify.own           auth
org.freedesktop.NetworkManager.settings.modify.system        auth
org.freedesktop.NetworkManager.sleep-wake                   no
org.freedesktop.NetworkManager.wifi.scan                  auth
org.freedesktop.NetworkManager.wifi.share.open            no
org.freedesktop.NetworkManager.wifi.share.protected       no

```

Comandos útiles de NetworkManager

En la siguiente tabla, se enumeran los comandos `nmcli` clave abordados en esta sección:

Comando	Propósito
<code>nmcli dev status</code>	Muestra el estado de todas las interfaces de red arrojado por NetworkManager.
<code>nmcli con show</code>	Enumerar todas las conexiones.
<code>nmcli con show <i>name</i></code>	Enumera la configuración actual del nombre de la conexión.
<code>nmcli con add con-name <i>name</i></code>	Agrega y asigna un nombre a un nuevo perfil de conexión.
<code>nmcli con mod <i>name</i></code>	Modifica el nombre de la conexión.
<code>nmcli con reload</code>	Vuelva a cargar los archivos de configuración, después de la edición manual de archivos.
<code>nmcli con up <i>name</i></code>	Active el nombre de la conexión.
<code>nmcli dev dis <i>dev</i></code>	Desconecte la interfaz, que también desactiva la conexión actual.
<code>nmcli con del <i>name</i></code>	Elimine la conexión especificada y su archivo de configuración.



Referencias

Para obtener más información, consulte el capítulo *Getting Started with nmcli* en https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/configuring_and_managing_networking/index#getting-started-with-nmcli_configuring-and-managing-networking

Páginas del manual: `NetworkManager(8)`, `nmcli(1)`, `nmcli-examples(5)`, `nm-settings(5)`, `hostnamectl(1)`, `resolv.conf(5)`, `hostname(5)`, `ip(8)` y `ip-address(8)`.

► Ejercicio Guiado

Configuración de redes desde la línea de comandos

En este ejercicio, usará el comando `nmcli` para configurar la configuración de red.

Resultados

- Actualizar una configuración de conexión de red de DHCP a estática.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start net-configure
```

Instrucciones

- 1. Use el comando `ssh` para iniciar sesión en la máquina `servera` con el usuario `student`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

- 2. Visualización de la información de interfaz de red



Importante

Los nombres de la interfaz de red están determinados por su tipo de bus y el orden de detección de los dispositivos durante el arranque. Los nombres de la interfaz de red variarán según la plataforma del curso y el hardware en uso.

En su sistema, localice el nombre de la interfaz (como `eth1`, `ens06` o `enp0p2`) asociado a la dirección Ethernet `52:54:00:00:fa:0a`. Use este nombre de interfaz para reemplazar el marcador de posición `eth0` que se usa a lo largo de este ejercicio, en caso de ser diferente.

Localice el nombre de la interfaz de red asociado con la dirección Ethernet `52:54:00:00:fa:0a`. Registre o recuerde este nombre y utilícelo para reemplazar el marcador de posición `eth0` en los comandos subsiguientes.

```
[root@servera ~]# ip link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
    group default qlen 1000
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode
    DEFAULT group default qlen 1000
        link/ether 52:54:00:00:fa:0a brd ff:ff:ff:ff:ff:ff
        altname enp0s3
        altname ens3
```

- 3. Use el comando `nmcli` para ver la configuración de red.

- 3.1. Use `nmcli con show` para mostrar todas las conexiones.

```
[root@servera ~]# nmcli con show
NAME           UUID                                  TYPE      DEVICE
System eth0   5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03  ethernet  eth0
System eth1   9c92fad9-6ecb-3e6c-eb4d-8a47c6f50c04  ethernet  --
```

- 3.2. Use el comando `nmcli con show --active` para mostrar solo las conexiones activas.

Su nombre de interfaz de red debe aparecer debajo de la columna **DEVICE** de los resultados, y el nombre de la conexión activa para ese dispositivo aparece en la misma línea debajo de la columna **NAME**. Este ejercicio asume que la conexión activa es `System eth0`. Si el nombre de la conexión activa es diferente, use ese nombre en lugar de `System eth0` para el resto de este ejercicio.

```
[root@servera ~]# nmcli con show --active
NAME           UUID                                  TYPE      DEVICE
System eth0   03da038a-3257-4722-a478-53055cc90128  ethernet  eth0
```

- 3.3. Muestre todos los parámetros de configuración para la conexión activa.

```
[root@servera ~]# nmcli con show "System eth0"
connection.id:          System eth0
connection.uuid:         5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03
connection.stable-id:    --
connection.type:         802-3-ethernet
connection.interface-name: eth0
connection.autoconnect:  yes
...output omitted...
ipv4.method:            manual
ipv4.dns:                172.25.250.254,2.2.2.2
ipv4.dns-search:         lab.example.com,example.com
ipv4.dns-options:       --
ipv4.dns-priority:      0
ipv4.addresses:          172.25.250.10/24
ipv4.gateway:            172.25.250.254
...output omitted...
ipv6.method:             ignore
ipv6.dns:                --
```

```

ipv6.dns-search:          --
ipv6.dns-options:         --
ipv6.dns-priority:        0
ipv6.addresses:           --
ipv6.gateway:             --
ipv6.routes:              --
...output omitted...
GENERAL.NAME:             System eth0
GENERAL.UUID:              5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03
GENERAL.DEVICES:           eth0
GENERAL.IP-IFACE:          eth0
GENERAL.STATE:             activated
GENERAL.DEFAULT:            yes

```

3.4. Muestre el estado del dispositivo.

```
[root@servera ~]# nmcli dev status
DEVICE  TYPE      STATE      CONNECTION
eth0    ethernet  connected  System eth0
lo     loopback  unmanaged  --
```

3.5. Muestre los parámetros de configuración para el dispositivo eth0.

```
[root@servera ~]# nmcli dev show eth0
GENERAL.DEVICE:             eth0
GENERAL.TYPE:                ethernet
GENERAL.HWADDR:              52:54:00:00:FA:0A
GENERAL.MTU:                 1500
GENERAL.STATE:               100 (connected)
GENERAL.CONNECTION:          System eth0
GENERAL.CON-PATH:            /org/freedesktop/NetworkManager/ActiveConnection/3
WIRED-PROPERTIES.CARRIER:   on
IP4.ADDRESS[1]:              172.25.250.10/24
IP4.GATEWAY:                 172.25.250.254
IP4.ROUTE[1]:                dst = 172.25.250.0/24, nh = 0.0.0.0, mt = 100
IP4.ROUTE[2]:                dst = 0.0.0.0/0, nh = 172.25.250.254, mt = 100
IP4.DNS[1]:                  172.25.250.254
IP4.SEARCHES[1]:              lab.example.com
IP4.SEARCHES[2]:              example.com
IP6.ADDRESS[1]:              fe80::5054:ff:fe00:fa0a/64
IP6.GATEWAY:                 --
IP6.ROUTE[1]:                dst = fe80::/64, nh = ::, mt = 256
```

- ▶ 4. Cree una conexión estática con la misma dirección IPv4, prefijo de red y puerta de enlace predeterminada que la conexión activa. Asigne el nombre **static-addr** a la conexión nueva.

**Advertencia**

Dado que el acceso al equipo se logra a través de la conexión de red principal, configurar los valores incorrectos durante la configuración de red puede hacer que su equipo no pueda encontrarse. Si no puede encontrar su máquina, use el botón **Reset** que está arriba de lo que antes era la pantalla gráfica del equipo e inténtelo de nuevo.

```
[root@servera ~]# nmcli con add con-name static-addr \
  ifname eth0 type ethernet ipv4.method manual \
  ipv4.addresses 172.25.250.10/24 ipv4.gateway 172.25.250.254
Connection 'static-addr' (c242697d-498e-481c-b974-5ae11d2a0291) successfully
added.
```

- 5. Modifique la conexión nueva para agregar el parámetro de configuración DNS.

```
[root@servera ~]# nmcli con mod static-addr ipv4.dns 172.25.250.254
```

- 6. Muestre y active la conexión nueva.

- 6.1. Visualice todas las conexiones.

```
[root@servera ~]# nmcli con show
NAME           UUID                                  TYPE      DEVICE
System eth0    5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03  ethernet  eth0
static-addr   e4cf52d3-40fc-41b3-b5e8-cf280157f3bb  ethernet  --
System eth1    9c92fad9-6ecb-3e6c-eb4d-8a47c6f50c04  ethernet  --
```

- 6.2. Visualice las conexiones activas.

```
[root@servera ~]# nmcli con show --active
NAME           UUID                                  TYPE      DEVICE
System eth0    5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03  ethernet  eth0
```

- 6.3. Active la nueva conexión static-addr.

```
[root@servera ~]# nmcli con up static-addr
Connection successfully activated (D-Bus active path: /org/freedesktop/
NetworkManager/ActiveConnection/4)
```

- 6.4. Verifique la nueva conexión activa.

```
[root@servera ~]# nmcli con show --active
NAME           UUID                                  TYPE      DEVICE
static-addr   e4cf52d3-40fc-41b3-b5e8-cf280157f3bb  ethernet  eth0
```

- 7. Actualice la conexión anterior para que no se inicie en el arranque. Verifique que se use la conexión **static-addr** cuando se reinicie el sistema.

71. Deshabilite la conexión original para que no se inicie automáticamente en el arranque.

```
[root@servera ~]# nmcli con mod "System eth0" \
connection.autoconnect no
```

72. Reinicie el sistema.

```
[root@servera ~]# systemctl reboot
Connection to servera closed by remote host.
Connection to servera closed.
[student@workstation ~]$
```

73. Inicie sesión en la máquina **servera** y verifique que la conexión **static-addr** sea la conexión activa.

```
[student@workstation ~]$ ssh student@servera
[student@servera ~]$ nmcli con show --active
NAME           UUID                                  TYPE      DEVICE
static-addr    e4cf52d3-40fc-41b3-b5e8-cf280157f3bb  ethernet  eth0
```

► 8. Pruebe la conectividad con las direcciones de red nuevas.

8.1. Verifique la dirección IP.

```
[student@servera ~]$ ip -br addr show eth0
eth0      UP            172.25.250.10/24 fe80::47cd:2076:4a6b:e730/64
```

8.2. Verifique la puerta de enlace predeterminada.

```
[student@servera ~]$ ip route
default via 172.25.250.254 dev eth0 proto static metric 100
172.25.250.0/24 dev eth0 proto kernel scope link src 172.25.250.10 metric 100
```

8.3. Compruebe la dirección DNS.

```
[student@servera ~]$ ping -c3 172.25.250.254
PING 172.25.250.254 (172.25.250.254) 56(84) bytes of data.
64 bytes from 172.25.250.254: icmp_seq=1 ttl=64 time=0.669 ms
64 bytes from 172.25.250.254: icmp_seq=2 ttl=64 time=0.294 ms
64 bytes from 172.25.250.254: icmp_seq=3 ttl=64 time=0.283 ms

--- 172.25.250.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2035ms
rtt min/avg/max/mdev = 0.283/0.415/0.669/0.179 ms
```

8.4. Regrese al sistema **workstation** como el usuario **student**.

```
[student@servera ~]$ exit  
logout  
Connection to servera closed.  
[student@workstation ~]$
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish net-configure
```

Esto concluye la sección.

Edición de archivos de configuración de red

Objetivos

Modificar la configuración de la red mediante la edición de los archivos de configuración.

Archivos de configuración de conexión

A partir de Red Hat Enterprise Linux 8, las configuraciones de red se almacenan en el directorio `/etc/NetworkManager/system-connections/`. Esta nueva ubicación de configuración usa el formato de archivo de claves en lugar del formato `ifcfg`. Sin embargo, las configuraciones almacenadas anteriormente en `/etc/sysconfig/network-scripts/` continúan funcionando. El directorio `/etc/NetworkManager/system-connections/` almacena cualquier cambio con el comando `nmcli con mod name`.

Formato de archivo de claves

NetworkManager usa el formato de clave de estilo INI para almacenar perfiles de conexión de red. Los pares de claves-valores almacenan configuraciones como secciones (grupos). Cada par de clave/valor de configuración en la sección es una de las propiedades enumeradas en la especificación de configuración. Este archivo de configuración almacena la mayoría de las configuraciones en el mismo formato que el formato de estilo INI. Por ejemplo, escribir direcciones IP como `192.168.0.1/24` es más fácil de leer que como matrices de números enteros.

Si bien la forma recomendada de administrar perfiles es con el comando `nmcli`, los usuarios aún pueden crear o modificar manualmente los archivos de configuración. Después de editar el archivo de configuración, ejecute el comando `nmcli con reload` para informar a NetworkManager acerca de estos cambios.

Comparación de la configuración de NetworkManager y el archivo de formato de archivo de claves

<code>nmcli con mod</code>	<code>* .nmconnection archivo</code>	Efecto
<code>ipv4.method manual</code>	<code>[ipv4]</code> <code>method=manual</code>	Las direcciones IPv4 se configuran de manera estática.
<code>ipv4.method auto</code>	<code>[ipv4]</code> <code>method=auto</code>	Busque parámetros de configuración de un servidor DHCPv4. No se muestra ninguna dirección estática hasta que tenga información de DHCPv4.

nmcli con mod	* .nmconnection archivo	Efecto
ipv4.addresses 192.0.2.1/24	[ipv4] address1=192.0.2.1/24	Establezca direcciones IPv4 estáticas y prefijos de red. Para más de una dirección de conexión, la tecla address2 define la segunda dirección y la tecla address3 define la tercera dirección.
ipv4.gateway 192.0.2.254	[ipv4] gateway=192.0.2.254	Establezca la puerta de enlace predeterminada.
ipv4.dns 8.8.8.8	[ipv4] dns=8.8.8.8	Modifique /etc/resolv.conf para que use este nombre de servidor.
ipv4.dns-search example.com	[ipv4] dns-search=example.com	Modifique /etc/resolv.conf para que use este dominio en la directiva search.
ipv4.ignore-auto-dns true	[ipv4] ignore-auto-dns=true	Omita información del servidor DNS obtenida del servidor DHCP.
ipv6.method manual	[ipv6] method=manual	Las direcciones IPv6 se configuran de manera estática.
ipv6.method auto	[ipv6] method=auto	Configure los parámetros de red con SLAAC a partir de anuncios del enrutador.
ipv6.method dhcp	[ipv6] method=dhcp	Configure los parámetros de red con DHCPv6, pero no con SLAAC.
ipv6.addresses 2001:db8::a/64	[ipv6] address1=2001:db8::a/64	Establezca direcciones IPv6 estáticas y prefijos de red. Al usar más de una dirección para una conexión, la tecla address2 define la segunda dirección y la tecla address3 define la tercera dirección.
ipv6.gateway 2001:db8::1	[ipv6] gateway=2001:db8::1	Establezca la puerta de enlace predeterminada.
ipv6.dns fde2:6494:1e09:2::d	[ipv6] dns=fde2:6494:1e09:2::d	Modifique /etc/resolv.conf para que use este nombre de servidor. Igual que IPv4.

nmcli con mod	* .nmconnection archivo	Efecto
ipv6.dns-search example.com	[ipv6] dns-search=example.com	Modifique /etc/resolv.conf para que use este dominio en la directiva search.
ipv6.ignore-auto-dns true	[ipv6] ignore-auto-dns=true	Omita información del servidor DNS obtenida del servidor DHCP.
connection.autoconnect yes	[connection] autoconnect=true	Activa automáticamente esta conexión durante el arranque.
connection.id ens3	[connection] id>Main eth0	El nombre de esta conexión.
connection.interface-name ens3	[connection] interface-name=ens3	La conexión se limita a la interfaz de red con este nombre.
802-3-ethernet.mac-address ...	[802-3-ethernet] mac-address=	La conexión se limita a la interfaz de red con esta dirección MAC.

Modificación de la configuración de red

También puede configurar la red editando directamente los archivos de configuración de conexión. Los archivos de configuración de conexión controlan las interfaces de software para dispositivos de red individuales. En general, estos archivos se denominan /etc/sysconfig/network-scripts/*name*.nmconnection, donde *name* se refiere al nombre del dispositivo o a la conexión que controla el archivo de configuración.

Según el propósito del perfil de conexión, NetworkManager usa los siguientes directorios para almacenar los archivos de configuración:

- El directorio /etc/NetworkManager/system-connections/ almacena perfiles persistentes que el usuario creó y editó. NetworkManager los copia automáticamente en el directorio /etc/NetworkManager/system-connections/.
- El directorio /run/NetworkManager/system-connections/ almacena perfiles temporales, que se eliminan automáticamente cuando reinicia el sistema.
- El directorio /usr/lib/NetworkManager/system-connections/ almacena perfiles inmutables implementados previamente. Cuando edita un perfil de este tipo con la API de NetworkManager, NetworkManager copia este perfil en el almacenamiento persistente o temporal.

Contenido del archivo de configuración de muestra para la configuración de IPv4 estática:

```
[connection]
id>Main eth0
uuid=27afa607-ee36-43f0-b8c3-9d245cdc4bb3
type=802-3-ethernet
```

```
autoconnect=true

[ipv4]
method=auto

[802-3-ethernet]
mac-address=00:23:5a:47:1f:71
```

Opciones de configuración IPv4 para el formato de archivo clave

Estática	Dinámica	Cualquiera de las opciones
[ipv4] address1=172.25.0.10/24 gateway=172.25.0.254 dns=172.25.254.254	method=auto	[connection] interface-name=ens3 id=Main eth0 autoconnect=true uuid=f3e8(...)ad3e type=ether

Después de modificar los archivos de configuración, establezca permisos en el archivo de configuración para que el usuario `root` lea y modifique el archivo de configuración.

```
[root@host ~]# chown root:root /etc/NetworkManager/system-connections/"Main
eth0.nmconnection"
[root@host ~]# chmod 600 /etc/NetworkManager/system-connections/"Main
eth0.nmconnection"
```

Ejecute el comando `nmcli con reload` para que NetworkManager lea los cambios de configuración. Cuando la variable `autoconnect` en el perfil use el valor `false`, active la conexión.

```
[root@host ~]# nmcli con reload
[root@host ~]# nmcli con up "static-ens3"
```



Referencias

Páginas del manual: `nmcli(1)`, `nm-settings(5)` y `nm-settings-keyfile(5)`

Para obtener más información, consulte la *Manually Creating NetworkManager Profiles in Key File Format* en

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/configuring_and_managing_networking/assembly_manually-creating-networkmanager-profiles-in-key-file-format_configuring-and-managing-networking

► Ejercicio Guiado

Edición de archivos de configuración de red

En este ejercicio, modifica manualmente los archivos de configuración de red y se asegura de que la nueva configuración surta efecto.

Resultados

- Configurar direcciones de red adicionales en cada sistema.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start net-edit
```

Instrucciones

- 1. En la máquina `workstation`, use el comando `ssh` para iniciar sesión en la máquina `servera` como el usuario `student`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

- 2. Localice nombres de interfaz de red con el comando `ip link`.



Importante

Los nombres de la interfaz de red están determinados por su tipo de bus y el orden de detección de los dispositivos durante el arranque. Los nombres de la interfaz de red variarán según la plataforma del curso y el hardware en uso.

Localice el nombre de la interfaz de red asociado con la dirección Ethernet en su sistema. Registre o recuerde este nombre y utilícelo para reemplazar el marcador de posición `enX` en los comandos subsiguientes. La conexión activa se denomina `Wired connection 1` y la configuración se encuentra en el archivo `/etc/NetworkManager/system-connections/"Wired connection 1.nmconnection"`.

```
[student@servera ~]$ ip link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
    group default qlen 1000
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode
    DEFAULT group default qlen 1000
        link/ether 52:54:00:00:fa:0a brd ff:ff:ff:ff:ff:ff
        altname enp0s3
        altname ens3
[student@servera ~]$ nmcli con show --active
NAME           UUID                                  TYPE      DEVICE
Wired connection 1  a98933fa-25c0-36a2-b3cd-c056f41758fe  ethernet  eth0
[student@servera ~]$ ls /etc/NetworkManager/system-connections/
'Wired connection 1.nmconnection'
```

- 3. En la máquina servera, cambie al usuario root y luego edite el archivo `/etc/NetworkManager/system-connections/"Wired connection 1.nmconnection"` para agregar la dirección `10.0.1.1/24`.

- 3.1. Use el comando `sudo -i` para cambiar al usuario root.

```
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

- 3.2. Edite el archivo de configuración. Agregue la dirección `10.0.1.1/24` como la segunda dirección debajo de la primera dirección en el archivo.

```
[root@servera ~]# vim /etc/NetworkManager/system-connections/"Wired connection
1.nmconnection"
..output omitted...
[ipv4]
address1=172.25.250.10/24,172.25.250.254
address2=10.0.1.1/24
...output omitted...
```

- 4. Active la nueva dirección de red con el comando `nmcli`.

- 4.1. Vuelva a cargar los cambios en la configuración para que NetworkManager los lea.

```
[root@servera ~]# nmcli con reload
```

- 4.2. Active la conexión con los cambios.

```
[root@servera ~]# nmcli con up "Wired connection 1"
Connection successfully activated (D-Bus active path: /org/freedesktop/
NetworkManager/ActiveConnection/2)
```

- 5. Verifique que la nueva dirección IP se haya asignado correctamente.

```
[root@servera ~]# ip -br addr show enX
eth0:      UP      172.25.250.10/24 10.0.1.1/24 fe80::6fed:5a11:4ad4:1bcf/64
```

- 6. Regrese a la máquina workstation como el usuario student.

```
[root@servera ~]# exit
logout
[student@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$
```

- 7. En la máquina serverb, edite el archivo /etc/NetworkManager/system-connections/"Wired connection 1.nmconnection" para agregar una dirección 10.0.1.2/24y, luego, cargue la nueva configuración.

- 7.1. Inicie sesión en la máquina servera como el usuario student y cambie al usuario root.

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
[student@serverb ~]$ sudo -i
[sudo] password for student: student
[root@serverb ~]#
```

- 7.2. Edite el archivo de configuración. Agregue la dirección 10.0.1.2/24 como la segunda dirección debajo de la primera dirección en el archivo.

```
[root@serverb ~]# vim /etc/NetworkManager/system-connections/"Wired connection 1.nmconnection"
address1=172.25.250.11/24,172.25.250.254
address2=10.0.1.2/24
```

- 7.3. Vuelva a cargar los cambios en la configuración para que NetworkManager los lea.

```
[root@serverb ~]# nmcli con reload
```

- 7.4. Active la conexión con los cambios.

```
[root@serverb ~]# nmcli con up "Wired connection 1"
Connection successfully activated (D-Bus active path: /org/freedesktop/
NetworkManager/ActiveConnection/2)
```

- 7.5. Verifique que la nueva dirección IP se haya asignado correctamente.

```
[root@serverb ~]# ip -br addr show enX
eth0      UP      172.25.250.11/24 10.0.1.2/24 fe80::6be8:6651:4280:892c/64
```

- 8. Pruebe la conectividad entre las máquinas **servera** y **serverb** con las direcciones de red nuevas.

8.1. Desde la máquina **serverb**, haga ping a la nueva dirección de la máquina **servera**.

```
[root@serverb ~]# ping -c3 10.0.1.1
PING 10.0.1.1 (10.0.1.1) 56(84) bytes of data.
64 bytes from 10.0.1.1: icmp_seq=1 ttl=64 time=1.30 ms
64 bytes from 10.0.1.1: icmp_seq=2 ttl=64 time=0.983 ms
64 bytes from 10.0.1.1: icmp_seq=3 ttl=64 time=0.312 ms

--- 10.0.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.312/0.864/1.297/0.410 ms
```

8.2. Regrese a la máquina **workstation** como el usuario **student**.

```
[root@serverb ~]# exit
logout
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@workstation ~]$
```

8.3. Desde la máquina **servera**, con el usuario **student**, haga ping a la nueva dirección de la máquina **serverb**.

```
[student@workstation ~]$ ssh student@servera ping -c3 10.0.1.2
PING 10.0.1.2 (10.0.1.2) 56(84) bytes of data.
64 bytes from 10.0.1.2: icmp_seq=1 ttl=64 time=0.876 ms
64 bytes from 10.0.1.2: icmp_seq=2 ttl=64 time=0.310 ms
64 bytes from 10.0.1.2: icmp_seq=3 ttl=64 time=0.289 ms

--- 10.0.1.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2047ms
rtt min/avg/max/mdev = 0.289/0.491/0.876/0.271 ms
```

Finalizar

En la máquina **workstation**, cambie al directorio de inicio de usuario **student** y use el comando **lab** para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish net-edit
```

Esto concluye la sección.

Configuración de nombres de host y resolución de nombre

Objetivos

Configurar el nombre de host estático del servidor y su resolución de nombre, y probar los resultados.

Actualización del nombre de host del sistema

El comando `hostname` muestra o modifica provisoriamente el nombre del host totalmente calificado del sistema.

```
[root@host ~]# hostname  
host.example.com
```

Especifique un nombre del host estático en el archivo `/etc/hostname`. Se usa el comando `hostnamectl` para modificar este archivo y ver el nombre del host totalmente calificado del sistema. Si este archivo no existe, el nombre del host se establece mediante una consulta de DNS invertida cuando se asigna una dirección IP a la interfaz.

```
[root@host ~]# hostnamectl set-hostname host.example.com  
[root@host ~]# hostnamectl status  
Static hostname: host.example.com  
    Icon name: computer-vm  
    Chassis: vm #  
    Machine ID: 663e281edea34ffea297bd479a8f12b5  
    Boot ID: 74bf3a0a48d540998a74055a0fe38821  
    Virtualization: kvm  
Operating System: Red Hat Enterprise Linux 9.0 (Plow)  
    CPE OS Name: cpe:/o:redhat:enterprise_linux:9::baseos  
    Kernel: Linux 5.14.0-70.el9.x86_64  
    Architecture: x86-64  
Hardware Vendor: Red Hat  
Hardware Model: OpenStack Compute  
[root@host ~]# cat /etc/hostname  
host.example.com
```



Importante

En Red Hat Enterprise Linux 7 y posterior, el nombre de host estático se almacena en el archivo `/etc/hostname`. Red Hat Enterprise Linux 6 y versiones anteriores almacenan el nombre de host como variable en el archivo `/etc/sysconfig/network`.

Configuración de la resolución de nombre

El sistema de resolución de nombres se usa para convertir nombres de host en direcciones IP o viceversa. Determina dónde buscar en función de la configuración del archivo `/etc/`

`nsswitch.conf`. De manera predeterminada, intenta resolver la consulta usando primero el archivo `/etc/hosts`.

```
[root@host ~]# cat /etc/hosts
127.0.0.1      localhost localhost.localdomain localhost4 localhost4.localdomain4
::1            localhost localhost.localdomain localhost6 localhost6.localdomain6
172.25.254.254 classroom.example.com
172.25.254.254 content.example.com
```

El comando `getent hosts hostname` puede usarse para probar la resolución de nombre del host con el archivo `/etc/hosts`. Si no se encuentra una entrada en el archivo `/etc/hosts`, el sistema de resolución de nombres usa un servidor de nombres DNS para buscar el nombre de host. El archivo `/etc/resolv.conf` controla la forma en que se realiza esta consulta:

- **search**: Lista de nombres de dominio para probar con un nombre de host corto. Se debe establecer `search` o `domain` en el mismo archivo; si ambos están configurados, solo se aplica la última entrada. Consulte `resolv.conf(5)` para obtener más detalles.
- **nameserver**: 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 un servidor de nombre no funcione.

```
[root@host ~]# cat /etc/resolv.conf
# Generated by NetworkManager
domain example.com
search example.com
nameserver 172.25.254.254
```

NetworkManager usa los parámetros de configuración de DNS en los archivos de configuración de conexión para actualizar el archivo `/etc/resolv.conf`. Use el comando `nmcli` para modificar las conexiones.

```
[root@host ~]# nmcli con mod ID ipv4.dns IP
[root@host ~]# nmcli con down ID
[root@host ~]# nmcli con up ID
[root@host ~]# cat /etc/sysconfig/network-scripts/ifcfg-ID
...output omitted...
DNS1=8.8.8.8
...output omitted...
```

El comportamiento predeterminado del comando `nmcli con mod ID ipv4.dns IP` es reemplazar cualquier parámetro de configuración de DNS anterior con la lista de IP nueva provista. Un signo más (+) o menos (-) delante del comando `nmcli` con la opción `ipv4.dns` agrega o elimina una entrada individual, respectivamente.

```
[root@host ~]# nmcli con mod ID +ipv4.dns IP
```

Para agregar el servidor DNS con la dirección IP IPv6 de `2001:4860:4860::8888` a la lista de servidores de nombres para usar con la conexión `static-ens3`:

```
[root@host ~]# nmcli con mod static-ens3 +ipv6.dns 2001:4860:4860::8888
```

**nota**

Las configuraciones DNS IPv4 e IPv6 estáticas terminan todas como directivas `nameserver` en `/etc/resolv.conf`. En un sistema de pila (stack) doble, mantenga al menos un servidor de nombres IPv4 accesible y uno IPv6 en la lista (suponiendo un sistema de pila doble), en caso de problemas de red con cualquiera de las pilas.

Prueba de resolución de nombres DNS

El comando de host `HOSTNAME` puede probar la conectividad del servidor DNS.

```
[root@host ~]# host classroom.example.com
classroom.example.com has address 172.25.254.254
[root@host ~]# host 172.25.254.254
254.25.25.172.in-addr.arpa domain name pointer classroom.example.com.
```

**Importante**

DHCP reescribe automáticamente el archivo `/etc/resolv.conf` cuando se inician las interfaces, a menos que usted especifique `PEERDNS=no` en los archivos de configuración de interfaz correspondientes. Configure esta entrada con el comando `nmcli`.

```
[root@host ~]# nmcli con mod "static-ens3" ipv4.ignore-auto-dns yes
```

Use el comando de dig `HOSTNAME` para probar la conectividad del servidor DNS.

```
[root@host ~]# dig classroom.example.com

; <>> DiG 9.16.23-RH <>> classroom.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3451
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 13, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 947ea2a936353423c3bc0d5f627cc1ae7147460e10d2777c (good)
;; QUESTION SECTION:
;classroom.example.com. IN A

;; ANSWER SECTION:
classroom.example.com. 85326 IN A 172.25.254.254
...output omitted...
```

Los comandos `host` y `dig` no ven la configuración en el archivo `/etc/hosts`. Para probar el archivo `/etc/hosts`, use el comando `getent hosts HOSTNAME`.

```
[root@host ~]# getent hosts classroom.example.com  
172.25.254.254 classroom.example.com
```



Referencias

Páginas del manual: `nmc li(1)`, `hostnamectl(1)`, `hosts(5)`, `getent(1)`, `host(1)`, `dig(1)`, `getent(1)` y `resolv.conf(5)`

Para obtener más información, consulte la *Configuring and Managing Networking Guide* en

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/configuring_and_managing_networking/index

► Ejercicio Guiado

Configuración de nombres de host y resolución de nombre

En este ejercicio, configura manualmente el nombre de host estático del sistema, el archivo `/etc/hosts` y el sistema de resolución de nombres DNS.

Resultados

- Establecer un nombre de host personalizado.
- Configurar los ajustes de resolución de nombres.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start net-hostnames
```

Instrucciones

- 1. Inicie sesión en `servera` con el usuario `student` y cambie al usuario `root`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

- 2. Visualice la configuración del nombre del host actual.

- 2.1. Muestre el nombre del host actual.

```
[root@servera ~]# hostname
servera.lab.example.com
```

- 2.2. Muestre el estado del nombre del host. Tenga en cuenta el nombre de host temporal obtenido de DHCP o mDNS.

```
[root@servera ~]# hostnamectl status
  Static hostname: n/a
  Transient hostname: servera.lab.example.com
    Icon name: computer-vm
      Chassis: vm
    Machine ID: 63b272eae8d5443ca7aaa5593479b25f
      Boot ID: ef299e0e957041ee81d0617fc98ce5ef
```

```

Virtualization: kvm
Operating System: Red Hat Enterprise Linux 9.0 (Plow)
CPE OS Name: cpe:/o:redhat:enterprise_linux:9::baseos
Kernel: Linux 5.14.0-70.el9.x86_64
Architecture: x86-64
Hardware Vendor: Red Hat
Hardware Model: OpenStack Compute

```

- 3. Configure un nombre del host estático para que coincida con el nombre del host transitorio actual.

- 3.1. Cambie el nombre de host y el archivo de configuración del nombre de host.

```
[root@servera ~]# hostnamectl set-hostname \
servera.lab.example.com
```

- 3.2. Visualice el contenido del archivo /etc/hostname que proporciona el nombre del host al inicio de la red.

```
servera.lab.example.com
```

- 3.3. Muestre el estado del nombre del host. El nombre de host temporal no se muestra ahora que se configuró un nombre de host estático.

```

[root@servera ~]# hostnamectl status
Static hostname: servera.lab.example.com
Icon name: computer-vm
Chassis: vm
Machine ID: 63b272eae8d5443ca7aaa5593479b25f
Boot ID: ef299e0e957041ee81d0617fc98ce5ef
Virtualization: kvm
Operating System: Red Hat Enterprise Linux 9.0 (Plow)
CPE OS Name: cpe:/o:redhat:enterprise_linux:9::baseos
Kernel: Linux 5.14.0-70.el9.x86_64
Architecture: x86-64
Hardware Vendor: Red Hat
Hardware Model: OpenStack Compute

```

- 4. Cambie temporalmente el nombre del host a testname.

- 4.1. Cambie el nombre de host.

```
[root@servera ~]# hostname testname
```

- 4.2. Muestre el nombre del host actual.

```
[root@servera ~]# hostname
testname
```

- 4.3. Visualice el contenido del archivo /etc/hostname que proporciona el nombre del host al inicio de la red.

```
servera.lab.example.com
```

- 4.4. Reinicie el sistema.

```
[root@servera ~]# systemctl reboot
Connection to servera closed by remote host.
Connection to servera closed.
[student@workstation ~]$
```

- 4.5. Inicie sesión en servera con el usuario student y cambie al usuario root.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

- 4.6. Muestre el nombre del host actual.

```
[root@servera ~]# hostname
servera.lab.example.com
```

- 5. Agregue class como apodo local para el servidor del aula y asegúrese de poder hacer ping al servidor con ese apodo.

- 5.1. Busque la dirección IP de classroom.example.com.

```
[root@servera ~]# host classroom.example.com
classroom.example.com has address 172.25.254.254
```

- 5.2. Actualice el archivo /etc/hosts para agregar class para acceder a la dirección IP 172.25.254.254. En el siguiente ejemplo, se muestra el contenido esperado del archivo /etc/hosts.

```
[root@servera ~]# vim /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 classroom class
```

- 5.3. Busque la dirección IP de class.

```
[root@servera ~]# host class
Host class not found: 3(NXDOMAIN)
[root@servera ~]# getent hosts class
172.25.254.254 classroom.example.com classroom class
```

- 5.4. Use el comando ping para enviar paquetes al servidor class.

```
[root@servera ~]# 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=63 time=1.21
ms
64 bytes from classroom.example.com (172.25.254.254): icmp_seq=2 ttl=63 time=0.688
ms
64 bytes from classroom.example.com (172.25.254.254): icmp_seq=3 ttl=63 time=0.559
ms

--- classroom.example.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2046ms
rtt min/avg/max/mdev = 0.559/0.820/1.214/0.283 ms
```

5.5. Regrese al sistema `workstation` como el usuario `student`.

```
[root@servera ~]# exit
logout
[student@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish net-hostnames
```

Esto concluye la sección.

► Trabajo de laboratorio

Administración de redes

En este trabajo de laboratorio, configurará los parámetros de red en un servidor Red Hat Enterprise Linux.

Resultados

- Configurar dos direcciones IPv4 estáticas para la interfaz de red principal.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start net-review
```

Instrucciones

- Inicie sesión en la máquina `serverb` como el usuario `student`. Cambie al usuario `root`.
- Cree una conexión con una configuración de red estática con los parámetros de configuración que figuran en la tabla.

Parámetro	Configuración
Nombre de la conexión	lab
Nombre de la interfaz	enX (podría variar, use la interfaz que tiene 52:54:00:00:fa:0b como dirección MAC)
dirección IP	172.25.250.11/24
Dirección de puerta de enlace	172.25.250.254
Dirección DNS	172.25.250.254

- Configure la nueva conexión para que se inicie automáticamente. Otras conexiones no deberían iniciarse automáticamente.
- Modifique la conexión nueva para que también use la dirección IP 10.0.1.1/24.
- Configure el archivo `hosts` para que pueda hacer referencia a la dirección IP 10.0.1.1 con el nombre `private`.
- Reinicie el sistema.
- Verifique que la máquina `serverb` esté inicializada.

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `Lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade net-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `Lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish net-review
```

Esto concluye la sección.

► Solución

Administración de redes

En este trabajo de laboratorio, configurará los parámetros de red en un servidor Red Hat Enterprise Linux.

Resultados

- Configurar dos direcciones IPv4 estáticas para la interfaz de red principal.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start net-review
```

Instrucciones

- Inicie sesión en la máquina `serverb` como el usuario `student`. Cambie al usuario `root`.
 - Inicie sesión en la máquina `serverb` como el usuario `student` y cambie al usuario `root`.

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
[student@serverb ~]$ sudo -i
[sudo] password for student: student
[root@serverb ~]#
```

- Cree una conexión con una configuración de red estática con los parámetros de configuración que figuran en la tabla.

Parámetro	Configuración
Nombre de la conexión	lab
Nombre de la interfaz	enX (podría variar, use la interfaz que tiene 52:54:00:00:fa:0b como dirección MAC)
dirección IP	172.25.250.11/24
Dirección de puerta de enlace	172.25.250.254
Dirección DNS	172.25.250.254

Determine el nombre de la interfaz y el nombre de la conexión activa actual. La solución asume que el nombre de la interfaz es `eth0` y el nombre de la conexión es `System eth0`.

```
[root@serverb ~]# ip link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
    group default qlen 1000
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode
    DEFAULT group default qlen 1000
        link/ether 52:54:00:00:fa:0b brd ff:ff:ff:ff:ff:ff
        altname enp0s3
        altname ens3
[root@serverb ~]# nmcli con show --active
NAME           UUID             TYPE      DEVICE
System eth0   5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03  ethernet  eth0
```

Cree el perfil de conexión `lab` basado en la información en la tabla descrita en las instrucciones. Asocie el perfil con el nombre de su interfaz de red que aparece en el resultado del comando `ip link` anterior.

```
[root@serverb ~]# nmcli con add con-name lab iface eth0 type ethernet \
    ipv4.method manual \
    ipv4.addresses 172.25.250.11/24 ipv4.gateway 172.25.250.254
[root@serverb ~]# nmcli con mod "lab" ipv4.dns 172.25.250.254
```

- Configure la nueva conexión para que se inicie automáticamente. Otras conexiones no deberían iniciarse automáticamente.

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

- Modifique la conexión nueva para que también use la dirección IP `10.0.1.1/24`.

```
[root@serverb ~]# nmcli con mod "lab" +ipv4.addresses 10.0.1.1/24
```

O bien, edite el archivo de configuración para agregar la dirección `10.0.1.1/24` como la segunda dirección.

```
[root@serverb ~]# vim /etc/NetworkManager/system-connections/lab.nmconnection
address2=10.0.1.1/24
```

- Configure el archivo `hosts` para que pueda hacer referencia a la dirección IP `10.0.1.1` con el nombre `private`.

```
[root@serverb ~]# echo "10.0.1.1 private" >> /etc/hosts
```

6. Reinicie el sistema.

```
[root@serverb ~]# systemctl reboot
Connection to serverb closed by remote host.
Connection to serverb closed.
[student@workstation ~]$
```

7. Verifique que la máquina `serverb` esté inicializada.

```
[student@workstation ~]$ ping -c3 serverb
PING serverb.lab.example.com (172.25.250.11) 56(84) bytes of data.
64 bytes from serverb.lab.example.com (172.25.250.11): icmp_seq=1 ttl=64
time=0.478 ms
64 bytes from serverb.lab.example.com (172.25.250.11): icmp_seq=2 ttl=64
time=0.504 ms
64 bytes from serverb.lab.example.com (172.25.250.11): icmp_seq=3 ttl=64
time=0.513 ms
--- serverb.lab.example.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 78ms
rtt min/avg/max/mdev = 0.478/0.498/0.513/0.023 ms
```

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade net-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish net-review
```

Esto concluye la sección.

Resumen

- El daemon `NetworkManager` monitorea y administra la configuración de la red.
- El comando `nmcli` es una herramienta de la línea de comandos para controlar la configuración de red con el daemon `NetworkManager`.
- A partir de Red Hat Enterprise Linux 9, la ubicación predeterminada para las configuraciones de red es el directorio `/etc/NetworkManager/system-connections`.
- El nombre del host estático del sistema se guarda en el archivo `/etc/hostname`.
- El comando `hostnamectl` modifica o ve el estado del nombre de host del sistema y los parámetros relacionados.

capítulo 14

Acceso al almacenamiento conectado a la red

Meta

Acceder al almacenamiento conectado a la red con el protocolo NFS.

Objetivos

- Identificar la información de exportación de NFS, crear un directorio para usar como punto de montaje, montar una exportación de NFS con el comando `mount` o mediante la configuración del archivo `/etc/fstab` y desmonte una exportación de NFS con el comando `umount`.
- Describir los beneficios de usar el servicio de automontaje y las exportaciones de NFS de automontaje mediante el uso de asignaciones directas e indirectas.

Secciones

- Administración de almacenamiento conectado a la red con NFS (y ejercicio guiado)
- Montaje automático de almacenamiento conectado a la red (y ejercicio guiado)

Trabajo de laboratorio

Acceso al almacenamiento conectado a la red

Administración de almacenamiento conectado a la red con NFS

Objetivos

Identificar la información de exportación de NFS, crear un directorio para usar como punto de montaje, montar una exportación de NFS con el comando `mount` o mediante la configuración del archivo `/etc/fstab` y desmonte una exportación de NFS con el comando `umount`.

Acceso a directorios NFS exportados

El *sistema de archivos de red* (NFS) es un protocolo estándar de Internet que usan Linux, UNIX y sistemas operativos similares como su sistema de archivos de red nativo. NFS es un estándar abierto que soporta permisos nativos de Linux y atributos del sistema de archivos.

De forma predeterminada, Red Hat Enterprise Linux 9 usa la versión 4.2 de NFS. RHEL soporta totalmente los protocolos NFSv3 y NFSv4. NFSv3 puede usar un protocolo de transporte TCP o UDP, pero NFSv4 solo permite conexiones TCP.

Los servidores NFS *exportan* directorios. Los clientes NFS montan directorios exportados en un directorio de punto de montaje local existente. Los clientes NFS pueden montar directorios exportados de varias maneras:

- **Manualmente**, con el comando `mount`.
- **De forma persistente en el arranque** mediante la configuración de entradas en el archivo `/etc/fstab`.
- **A pedido** mediante la configuración de un método de automontaje.

Los métodos de automontaje, que incluyen el servicio `autofs` y la utilidad `systemd.automount`, se analizan en la sección **Automount Network-Attached Storage**. Debe instalar el paquete `nfs-utils` para obtener las herramientas de cliente para el montaje manual, o para el automontaje, para obtener directorios NFS exportados.

```
[root@host ~]# dnf install nfs-utils
```

RHEL también soporta el montaje de directorios *compartidos* desde sistemas Microsoft Windows mediante el uso de los mismos métodos que para el protocolo NFS, mediante el uso de los protocolos Server Message Block (SMB) o Common Internet File System (CIFS). Las opciones de montaje son específicas del protocolo y dependen de la configuración de Windows Server o Samba Server.

Consultar los directorios NFS exportados de un servidor

El protocolo NFS cambió significativamente entre NFSv3 y NFSv4. El método para consultar un servidor para ver las exportaciones disponibles es diferente para cada versión de protocolo.

NFSv3 usó el protocolo RPC, que requiere un servidor de archivos que soporta conexiones NFSv3 para ejecutar el servicio `rpcbind`. Un cliente NFSv3 se conecta al servicio `rpcbind` en el puerto 111 en el servidor para solicitar el servicio NFS. El servidor responde con el puerto actual para el servicio NFS. Use el comando `showmount` para consultar las exportaciones disponibles en un servidor NFSv3 basado en RPC.

```
[root@host ~]# showmount --exports server
Export list for server
/shares/test1
/shares/test2
```

El protocolo NFSv4 eliminó el uso del protocolo RPC heredado para las transacciones NFS. El uso del comando `showmount` en un servidor que soporta solo el tiempo de espera de NFSv4 sin recibir una respuesta, ya que el servicio `rpcbind` no se está ejecutando en el servidor. Sin embargo, consultar un servidor NFSv4 es más sencillo que consultar un servidor NFSv3.

NFSv4 introdujo un *árbol de exportación* que contiene todas las rutas para los directorios exportados del servidor. Para ver todos los directorios exportados, monte la raíz (root) (/) del árbol de exportación del servidor. Montar la raíz (root) del árbol de exportación proporciona rutas navegables para todos los directorios exportados, como elementos secundarios del directorio raíz del árbol, pero no monta ("vincula") ninguno de los directorios exportados.

```
[root@host ~]# mkdir /mountpoint
[root@host ~]# mount server:/ /mountpoint
[root@host ~]# ls /mountpoint
```

Para montar una exportación de NFSv4 mientras navega por el árbol de exportación montado, cambie el directorio por una ruta de directorio exportado. De manera alternativa, use el comando `mount` con el nombre de ruta completo de un directorio exportado para montar un único directorio exportado. Los directorios exportados que usan la seguridad de Kerberos no permiten montar o acceder a un directorio mientras se explora un árbol de exportación, aunque puede ver el nombre de la ruta de exportación. El montaje de recursos compartidos protegidos por Kerberos requiere una configuración de servidor adicional y el uso de credenciales de usuario de Kerberos, que se analizan en el curso de capacitación Red Hat Security: Identity Management and Active Directory Integration (RH362).

Montaje manual de directorios NFS exportados

Después de identificar la exportación de NFS que se montará, cree un punto de montaje local si aún no existe. El directorio `\mnt` está disponible para su uso como punto de montaje temporal, pero la práctica recomendada es no usar `\mnt` para el montaje a largo plazo o persistente.

```
[root@host ~]# mkdir /mountpoint
```

Al igual que con los sistemas de archivos de volúmenes locales, monte la exportación de NFS para acceder a su contenido. Los recursos compartidos de NFS pueden montarse de forma temporal o permanente, solo por un usuario con privilegios.

```
[root@host ~]# mount -t nfs -o rw,sync server:/export /mountpoint
```

La opción `-t nfs` especifica el tipo de sistema de archivos NFS. Sin embargo, cuando el comando `mount` detecta la sintaxis `server:/export`, el comando toma el tipo NFS de manera predeterminada. La opción `-o sync` especifica que todas las transacciones al sistema de archivos exportado se realizan de forma sincrónica, lo que se recomienda encarecidamente para todos los montajes de red de producción donde las transacciones deben completarse o, de lo contrario, se devuelven como fallidas.

El uso de un comando manual `mount` no es persistente. Cuando se reinicia el sistema, esa exportación de NFS aún no se montará. Los montajes manuales son útiles para proporcionar acceso temporal a un directorio exportado o para probar el montaje de una exportación de NFS antes de montarla de forma persistente.

Montaje de manera persistente de directorios NFS exportados

Para montar de forma persistente una exportación de NFS, edite el archivo `/etc/fstab` y agregue la entrada de montaje con una sintaxis similar al montaje manual.

```
[root@host ~]# vim /etc/fstab
...
server:/export  /mountpoint  nfs  rw,soft  0 0
```

A continuación, puede montar la exportación de NFS usando solo el punto de montaje. El comando `mount` obtiene el servidor NFS y las opciones de montaje de la entrada coincidente en el archivo `/etc/fstab`.

```
[root@host ~]# mount /mountpoint
```

Desmontaje de directorios NFS exportados

Como usuario privilegiado, desmonte una exportación de NFS con el comando `umount`. Desmontar un recurso compartido no elimina su entrada en el archivo `/etc/fstab` si existe. Las entradas en el archivo `/etc/fstab` son persistentes y se vuelven a montar durante el arranque.

```
[root@host ~]# umount /mountpoint
```

Un directorio montado a veces puede fallar al desmontar y devuelve un error que el `device is busy`. El dispositivo está ocupado porque una aplicación mantiene un archivo abierto dentro del sistema de archivos o porque la shell de algún usuario tiene un directorio de trabajo en el directorio root del sistema de archivos montado o debajo de él.

Para resolver el error, verifique sus propias ventanas de shell activas y use el comando `cd` para dejar el sistema de archivos montado. Si los intentos posteriores de desmontar el sistema de archivos aún fallan, use el comando `lsof` (*enumerar archivos abiertos*) para consultar el punto de montaje. El comando `lsof` devuelve una lista de nombres de archivos abiertos y el proceso que mantiene el archivo abierto.

```
[root@host ~]# lsof /mountpoint
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
program 5534 user txt REG 252.4 910704 128 /home/user/program
```

Con esta información, cierre correctamente cualquier proceso que esté usando archivos en este sistema de archivos y vuelva a intentar el desmontaje. Solo en escenarios críticos, cuando una aplicación no se puede cerrar correctamente, finalice el proceso para cerrar el archivo. De manera alternativa, use la opción `umount -f` para forzar el desmontaje, que puede causar la pérdida de datos no escritos para todos los archivos abiertos.



Referencias

Páginas del manual: `mount(8)`, `umount(8)`, `showmount(8)`, `fstab(5)`,
`mount.nfs(8)`, `nfsconf(8)` y `rpcbind(8)`

► Ejercicio Guiado

Administración de almacenamiento conectado a la red con NFS

Lista de verificación de rendimiento

En este ejercicio, modifica el archivo /etc/fstab para montar de forma persistente una exportación de NFS en el momento del arranque.

Resultados

- Probar un servidor NFS con el comando `mount`.
- Configurar exportaciones de NFS en el archivo de configuración /etc/fstab para guardar los cambios incluso después de reiniciar el sistema.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start netstorage-nfs
```

Instrucciones

Una empresa de transporte usa un servidor NFS central, `serverb`, para alojar diversos documentos y directorios exportados. Los usuarios de `servera`, que son todos miembros del grupo `admin`, necesitan acceso a la exportación NFS montada de forma persistente.

Características del entorno:

- La máquina `serverb` exporta el directorio `/shares/public`, que contiene algunos archivos de texto.
- Los miembros del grupo `admin` (`admin1`, `sysmanager1`) tienen acceso de lectura y escritura al directorio exportado `/shares/public`.
- El punto de montaje en `servera` debe ser el directorio `/public`.
- Todas las contraseñas de usuario están definidas en `redhat`.
- El paquete `nfs-utils` ya esté instalado.

► 1. Inicie sesión en `servera` como el usuario `student` y cambie al usuario `root`.

- 1.1. Inicie sesión en `servera` como el usuario `student` y cambie al usuario `root`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

► 2. Pruebe el servidor NFS en serverb con servera como cliente NFS.

- 2.1. Cree el punto de montaje /public en la máquina servera.

```
[root@servera ~]# mkdir /public
```

- 2.2. En servera, verifique que la exportación de NFS /share/public de serverb se monte correctamente en el directorio /public.

```
[root@servera ~]# mount -t nfs \
serverb.lab.example.com:/shares/public /public
```

- 2.3. Enumere el contenido de la exportación de NFS montado.

```
[root@servera ~]# ls -l /public
total 16
-rw-r--r-- 1 root admin 42 Apr  8 22:36 Delivered.txt
-rw-r--r-- 1 root admin 46 Apr  8 22:36 NOTES.txt
-rw-r--r-- 1 root admin 20 Apr  8 22:36 README.txt
-rw-r--r-- 1 root admin 27 Apr  8 22:36 Trackings.txt
```

- 2.4. Explore las opciones de comando mount para la exportación de NFS montado.

```
[root@servera ~]# mount | grep public
serverb.lab.example.com:/shares/public on /public type nfs4
(rw,relatime,vers=4.2,rsize=262144,wsize=262144,namlen=255,sync
,proto=tcp,timeo=600,retrans=2,sec=sys,clientaddr=172.25.250.10,
local_lock=none,addr=172.25.250.11)
```

- 2.5. Desmonte la exportación de NFS.

```
[root@servera ~]# umount /public
```

► 3. Configure servera para que la exportación /share/public se monte de forma persistente.

- 3.1. Edite el archivo /etc/fstab.

```
[root@servera ~]# vim /etc/fstab
```

Agregue la línea siguiente al final del archivo:

```
serverb.lab.example.com:/shares/public /public nfs rw,sync 0 0
```

3.2. Monte el directorio exportado.

```
[root@servera ~]# mount /public
```

3.3. Enumere el contenido del directorio exportado.

```
[root@servera ~]# ls -l /public
total 16
-rw-r--r--. 1 root    admin 42 Apr  8 22:36 Delivered.txt
-rw-r--r--. 1 root    admin 46 Apr  8 22:36 NOTES.txt
-rw-r--r--. 1 root    admin 20 Apr  8 22:36 README.txt
-rw-r--r--. 1 root    admin 27 Apr  8 22:36 Trackings.txt
```

3.4. Reinicie la máquina servera.

```
[root@servera ~]# systemctl reboot
```

- 4. Una vez que servera haya finalizado el reinicio, inicie sesión en servera con el usuario admin1 y pruebe la exportación de NFS montado de forma persistente.

4.1. Inicie sesión en servera con el usuario admin1.

```
[student@workstation ~]$ ssh admin1@servera
[admin1@servera ~]$
```

4.2. Pruebe la exportación de NFS que está montada en el directorio /public.

```
[admin1@servera ~]$ ls -l /public
total 16
-rw-r--r--. 1 root    admin 42 Apr  8 22:36 Delivered.txt
-rw-r--r--. 1 root    admin 46 Apr  8 22:36 NOTES.txt
-rw-r--r--. 1 root    admin 20 Apr  8 22:36 README.txt
-rw-r--r--. 1 root    admin 27 Apr  8 22:36 Trackings.txt
[admin1@servera ~]$ cat /public/NOTES.txt
###In this file you can log all your notes###
[admin1@servera ~]$ echo "This is a test" > /public/Test.txt
[admin1@servera ~]$ cat /public/Test.txt
This is a test
```

4.3. Regrese a la máquina workstation como el usuario student.

```
[admin1@servera ~]$ exit
logout
Connection to servera closed.
```

Finalizar

En la máquina workstation, cambie al directorio de inicio de usuario student y use el comando lab para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish netstorage-nfs
```

Esto concluye la sección.

Montaje automático de almacenamiento conectado a la red

Objetivos

Describir los beneficios de usar el servicio de automontaje y las exportaciones de NFS de automontaje mediante el uso de asignaciones directas e indirectas.

Montaje de exportaciones de NFS con el servicio de automontaje

El *automontaje* es un servicio (*autofs*) que monta automáticamente los sistemas de archivos y las exportaciones de NFS a pedido, y desmonta automáticamente los sistemas de archivos y las exportaciones de NFS cuando los recursos montados ya no están en uso.

La función de automontaje se creó para resolver el problema de que los usuarios sin privilegios no tienen permisos suficientes para usar el comando `mount`. Sin el uso del comando `mount`, los usuarios normales no pueden acceder a medios extraíbles como CD, DVD y unidades de disco extraíbles. Además, si un sistema de archivos local o remoto no se monta en el momento del arranque mediante la configuración `/etc/fstab`, un usuario normal no puede montar y acceder a esos sistemas de archivos desmontados.

Los archivos de configuración del servicio de automontaje se completan con información de montaje del sistema de archivos, de manera similar a las entradas `/etc/fstab`. Aunque los sistemas de archivos `/etc/fstab` se montan durante el arranque del sistema y permanecen montados hasta el apagado del sistema u otra intervención, los sistemas de archivos de automontaje no necesariamente se montan durante el arranque del sistema. En cambio, los sistemas de archivos controlados por el servicio de automontaje se montan a pedido, cuando un usuario o una aplicación intenta ingresar al punto de montaje del sistema de archivos para acceder a los archivos.

Beneficios del servicio de automontaje

El uso de recursos para los sistemas de archivos de automontaje es equivalente a los sistemas de archivos que se montan en el arranque, ya que un sistema de archivos usa recursos solo cuando un programa lee y escribe archivos abiertos. Los sistemas de archivos montados pero inactivos y los sistemas de archivos desmontados usan la misma cantidad de recursos: casi ninguno.

La ventaja del automontaje es que al desmontar el sistema de archivos cada vez que ya no está en uso, el sistema de archivos está protegido de daños inesperados mientras está abierto. Cuando se indica al sistema de archivos que se monte nuevamente, el servicio `autofs` usa la configuración de montaje más actual, a diferencia de un montaje `/etc/fstab`, que aún puede usar una configuración que se montó hace meses durante el último arranque del sistema. Además, si la configuración del servidor NFS incluye servidores y rutas redundantes, el servicio de automontaje puede seleccionar la conexión más rápida cada vez que se solicita un nuevo sistema de archivos.

Método de servicio `autofs` de automontaje

El servicio `autofs` soporta los mismos sistemas de archivos locales y remotos que en el archivo `/etc/fstab`, incluidos los protocolos de uso compartido de archivos NFS y SMB, y soporta las mismas opciones de montaje específicas del protocolo, incluidos los parámetros de seguridad. Los sistemas de archivos que se montan a través del programa de automontaje están disponibles de

manera predeterminada para todos los usuarios, pero se pueden restringir a través de las opciones de permisos de acceso.

Debido a que el servicio de automontaje es una configuración del lado del cliente que usa los comandos estándares `mount` y `umount` para administrar sistemas de archivos, los sistemas de archivos automontados en uso muestran un comportamiento idéntico a los sistemas de archivos que se montan con `/etc/fstab`. La diferencia es que un sistema de archivos de automontaje permanece desmontado hasta que se accede al punto de montaje, lo que hace que el sistema de archivos se monte inmediatamente y permanezca montado mientras el sistema de archivos está en uso. Cuando se cierran todos los archivos en el sistema de archivos, y todos los usuarios y procesos abandonan el directorio de punto de montaje, el servicio de automontaje desmonta el sistema de archivos después de un tiempo de espera mínimo.

Casos de uso de asignaciones directas e indirectas

El servicio de automontaje soporta la asignación directa e indirecta de puntos de montaje, para gestionar los dos tipos de montaje bajo demanda. Un montaje *directo* es cuando un sistema de archivos se monta en una ubicación de punto de montaje conocida que no cambia. Casi todos los montajes del sistema de archivos que configuró, antes de aprender sobre el automontaje, son ejemplos de montajes directos. Un punto de montaje *directo* existe como un directorio permanente, al igual que otros directorios normales.

Un montaje *indirecto* se produce cuando no se conoce la ubicación del punto de montaje hasta que se produce la demanda de montaje. Un ejemplo de montaje indirecto es la configuración para directorios de inicio montados de forma remota, donde el directorio de inicio de un usuario incluye su nombre de usuario en la ruta del directorio. El sistema de archivos remoto del usuario se monta en su directorio de inicio, solo después de que el programa de automontaje sepa qué usuario ha especificado montar su directorio de inicio y determina la ubicación del punto de montaje que se debe usar. Aunque los puntos de montaje *indirectos* parecen existir, el servicio `autofs` los crea cuando se produce la demanda de montaje y los elimina nuevamente cuando la demanda ha finalizado y se desmonta el sistema de archivos.

Configuración del servicio de automontaje

El proceso para configurar un automontaje tiene muchos pasos.

Primero debe instalar los paquetes `autofs` y `nfs-utils`.

```
[user@host ~]$ sudo dnf install autofs nfs-utils
```

Estos paquetes contienen todos los requisitos para usar el servicio de automontaje para las exportaciones de NFS.

Creación de una asignación maestra

A continuación, agregue un archivo de asignación maestra en `/etc/auto.master.d`. Este archivo identifica el directorio de base para puntos de montaje e identifica el archivo de asignación para crear los automontajes.

```
[user@host ~]$ sudo vim /etc/auto.master.d/demo.autofs
```

El nombre del archivo de asignación maestra es principalmente arbitrario (aunque suele tener un sentido) y debe tener una extensión de `.autofs` para que el subsistema lo reconozca. Puede colocar varias entradas en un solo archivo de asignación maestra; como alternativa, puede crear

varios archivos de asignación maestra, cada uno con sus propias entradas agrupadas de forma lógica.

Agregue la entrada de asignación maestra, en este caso, para montajes asignados indirectamente:

```
/shares /etc/auto.demo
```

Esta entrada usa 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`.

Creación de un mapa indirecto

Ahora, cree los archivos de asignación. Cada archivo de asignación identifica el punto de montaje, las opciones de montaje y la ubicación de origen que se montará para un conjunto de automontajes.

```
[user@host ~]$ sudo vim /etc/auto.demo
```

La convención de nomenclatura de archivos de asignación es `/etc/auto.name`, donde el *nombre* refleja el contenido de la asignación.

```
work -rw, sync serverb:/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 tratan más adelante en esta sección.

Conocido como la *clave* en las páginas del manual, el *punto de montaje* se crea y elimina automáticamente con el servicio `autofs`. En este caso, el punto de montaje totalmente calificado es `/shares/work` (consulte el archivo de asignación maestra). Los directorios `/shares` y `/shares/work` se crean y se eliminan según sea necesario mediante el servicio `autofs`.

En este ejemplo, el punto de montaje local duplica la estructura del directorio del servidor. Sin embargo, esta duplicación no es necesaria; el punto de montaje local puede tener un nombre arbitrario. El servicio `autofs` no impone (enforce) una estructura de nombres específica en el cliente.

Las opciones de montaje comienzan con un carácter de guión (-) y se separan por comas sin espacios en blanco. Las opciones de montaje de un sistema de archivos disponibles para el montaje manual también están disponibles al realizar el automontaje. En este ejemplo, el servicio de automontaje monta la exportación con acceso de lectura y escritura (opción `rw`) y el servidor se sincroniza inmediatamente durante las operaciones de escritura (opción `sync`).

Algunas opciones útiles específicas del servicio de automontaje son `-fstype=` y `-strict`. Use `fstype` para especificar el tipo de sistema de archivos, por ejemplo `nfs4` o `xfs`, y use `strict` para tratar errores como graves cuando monte sistemas de archivos.

La ubicación de origen para las exportaciones de NFS sigue el patrón `host:/pathname`; en este ejemplo, `serverb:/shares/work`. Para que este automontaje se realice correctamente, el servidor NFS, `serverb`, debe exportar el directorio con acceso de lectura y escritura, y el usuario que solicita el acceso debe tener permisos de archivo estándar de Linux en el directorio. Si `serverb` exporta el directorio con acceso de solo lectura, entonces el cliente obtendrá acceso de solo lectura a pesar de que solicitó acceso de lectura y escritura.

Comodines en una asignación indirecta

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.

Para continuar con el ejemplo anterior, si `serverb:/shares` exporta dos o más subdirectorios y se puede acceder a estos con las mismas opciones de montaje, el contenido del archivo `/etc/auto.demo` podría verse del siguiente modo:

```
* -rw, sync serverb:/shares/&
```

El punto de montaje (o clave) es un carácter de asterisco (*) y el subdirectorio en la ubicación de origen es el carácter de ampersand (&). Todo lo demás en la entrada es igual.

Cuando un usuario intenta acceder a `/shares/work`, la clave * (que es `work` en este ejemplo) reemplaza el ampersand en la ubicación de origen y se monta `serverb:/exports/work`. Al igual que con el ejemplo indirecto, el servicio `autofs` crea y elimina automáticamente el directorio `work`.

Creación de una asignación indirecta

Una asignación indirecta se usa para asignar una exportación de NFS a un punto de montaje de ruta absoluta. Solo se necesita un archivo de asignación directa, que puede contener cualquier cantidad de asignaciones directas.

Para usar puntos de montaje asignados directamente, el archivo de asignación maestra puede tener la siguiente apariencia:

```
/- /etc/auto.direct
```

Todas las entradas de asignación directa usan `/-` como el directorio de base. En este caso, el archivo de asignación que contiene los detalles de montaje es `/etc/auto.direct`.

El contenido del archivo `/etc/auto.direct` puede verse de la siguiente forma:

```
/mnt/docs -rw, sync serverb:/shares/docs
```

El punto de montaje (o clave) es siempre una ruta absoluta. El resto del archivo de asignación usa la misma estructura.

En este ejemplo, el directorio `/mnt` existe y no lo administra el servicio `autofs`. El servicio `autofs` crea y elimina automáticamente el directorio `/mnt/docs` completo.

Inicio del servicio de automontaje

Por último, use el comando `systemctl` para iniciar y habilitar el servicio `autofs`.

```
[user@host ~]$ sudo systemctl enable --now autofs
Created symlink /etc/systemd/system/multi-user.target.wants/autofs.service → /usr/
lib/systemd/system/autofs.service.
```

Método `systemd.automount` alternativo

El daemon `systemd` puede crear automáticamente archivos de unidad para entradas en `/etc/fstab` que incluyen la opción `x-systemd.automount`. Use el comando `systemctl daemon-reload` después de modificar las opciones de montaje de una entrada para generar un nuevo archivo de unidad y, luego, use el comando `systemctl start unit.automount` para habilitar esa configuración de automontaje.

El nombre de la unidad se basa en su ubicación de montaje. Por ejemplo, si el punto de montaje es `/remote/finance`, el archivo de la unidad se denomina `remote-finance.automount`. El daemon `systemd` monta el sistema de archivos cuando se accede inicialmente al directorio `/remote/finance`.

Este método puede ser más sencillo que instalar y configurar el servicio `autofs`. Sin embargo, una unidad `systemd.automount` puede soportar solo puntos de montaje de ruta absoluta, similar a las asignaciones directas `autofs`.



Referencias

Páginas del manual: `autofs(5)`, `automount(8)`, `auto.master(5)`, `mount.nfs(8)` y `systemd.automount(5)`

► Ejercicio Guiado

Montaje automático de almacenamiento conectado a la red

Lista de verificación de rendimiento

En este ejercicio, crea puntos de montaje de asignación directa y de asignación indirecta administrados por automontaje que montan sistemas de archivos NFS.

Resultados

- Instalar los paquetes necesarios para el servicio de automontaje.
- Configurar asignaciones directas e indirectas de automontaje con recursos de un servidor NFSv4 preconfigurado.
- Describir la diferencia entre las asignaciones directas e indirectas de automontaje.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este script de inicio determina si `servera` y `serverb` son accesibles en la red. El script le avisa si no están disponibles. El script de inicio configura `serverb` como servidor NFSv4, configura los permisos y exporta los directorios. El script también crea los usuarios y grupos necesarios en `servera` y `serverb`.

```
[student@workstation ~]$ lab start netstorage-autofs
```

Instrucciones

Un proveedor de servicios de Internet usa un servidor central, `serverb`, para alojar directorios compartidos con documentos importantes que deben estar disponibles a pedido. Cuando los usuarios inician sesión en `servera` necesitan acceso a los directorios compartidos de automontaje.

Características del entorno:

- La máquina `serverb` exporta el directorio `/shares/indirect`, que a su vez contiene los subdirectorios `west`, `central` y `east`.
- La máquina `serverb` también exporta el directorio `/shares/direct/external`.
- El grupo `operators` está compuesto por los usuarios `operator1` y `operator2`. Tienen acceso de lectura y escritura a los directorios exportados `/shares/indirect/west`, `/shares/indirect/central` y `/shares/indirect/east`.
- El grupo `contractors` está compuesto por los usuarios `contractor1` y `contractor2`. Tienen acceso de lectura y escritura al directorio exportado `/shares/direct/external`.
- Los puntos de montaje esperados para `servera` son `/externaly` y `/internal`.
- El directorio exportado `/shares/direct/external` se monta automáticamente en `servera` con una asignación `directa` en `/external`.
- El directorio exportado `/shares/indirect/west` debe montarse automáticamente en `servera` con una asignación `indirecta` en `/internal/west`.

capítulo 14 | Acceso al almacenamiento conectado a la red

- El directorio exportado `/shares/indirect/central` debe montarse automáticamente en `servera` con una asignación *indirecta* en `/internal/central`.
- El directorio exportado `/shares/indirect/east` debe montarse automáticamente en `servera` con una asignación *indirecta* en `/internal/east`.
- Todas las contraseñas de usuario están definidas en `redhat`.
- El paquete `nfs-utils` ya esté instalado.

► 1. Inicie sesión en `servera` e instale los paquetes requeridos.

1.1. Inicie sesión en `servera` como el usuario `student` y cambie al usuario `root`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

1.2. Instale el paquete `autofs`.

```
[root@servera ~]# dnf install autofs
...output omitted...
Is this ok [y/N]: y
...output omitted...
Complete!
```

► 2. Configure una asignación indirecta de automontaje en `servera` con los recursos exportados de `serverb`. Cree la asignación directa con los archivos denominados `/etc/auto.master.d/direct.autofs` para la asignación maestra y `/etc/auto.direct` para el archivo de asignación. Use el directorio `/external` como el punto de montaje principal en `servera`.

2.1. Pruebe el servidor NFS y exporte antes de configurar el servicio de automontaje.

```
[root@servera ~]# mount -t nfs \
serverb.lab.example.com:/shares/direct/external /mnt
[root@servera ~]# ls -l /mnt
total 4
-rw-r--r--. 1 root contractors 22 Apr  7 23:15 README.txt
[root@servera ~]# umount /mnt
```

2.2. Cree un archivo de asignación maestra llamado `/etc/auto.master.d/direct.autofs`, inserte el siguiente contenido y guarde los cambios.

```
/- /etc/auto.direct
```

2.3. Cree un archivo de asignación directa llamado `/etc/auto.direct`, inserte el siguiente contenido y guarde los cambios.

```
/external -rw,sync,fstype=nfs4 serverb.lab.example.com:/shares/direct/external
```

► 3. Configure una asignación indirecta de montaje automático en `servera` con los recursos exportados de `serverb`. Cree la asignación indirecta con los archivos denominados

capítulo 14 | Acceso al almacenamiento conectado a la red

/etc/auto.master.d/indirect.autofs para la asignación maestra y /etc/auto.indirect para el archivo de asignación. Use el directorio /internal como el punto de montaje principal en servera.

- 3.1. Pruebe el servidor NFS y exporte antes de configurar el servicio de automontaje.

```
[root@servera ~]# mount -t nfs \
serverb.lab.example.com:/shares/indirect /mnt
[root@servera ~]# ls -l /mnt
total 0
drwxrws--- 2 root operators 24 Apr  7 23:34 central
drwxrws--- 2 root operators 24 Apr  7 23:34 east
drwxrws--- 2 root operators 24 Apr  7 23:34 west
[root@servera ~]# umount /mnt
```

- 3.2. Cree un archivo de asignación maestra llamado /etc/auto.master.d/indirect.autofs, inserte el siguiente contenido y guarde los cambios.

```
/internal /etc/auto.indirect
```

- 3.3. Cree un archivo de asignación indirecta llamado /etc/auto.indirect, inserte el siguiente contenido y guarde los cambios.

```
* -rw, sync, fstype=nfs4 serverb.lab.example.com:/shares/indirect/&
```

- 4. Inicie el servicio `autofs` en servera y habilítelo para que se inicie automáticamente durante el proceso de arranque. Reinicie servera para determinar si el servicio `autofs` se inicia automáticamente.

- 4.1. Inicie y habilite el servicio `autofs` en servera.

```
[root@servera ~]# systemctl enable --now autofs
Created symlink /etc/systemd/system/multi-user.target.wants/autofs.service → /usr/
lib/systemd/system/autofs.service.
```

- 4.2. Reinicie la máquina servera.

```
[root@servera ~]# systemctl reboot
```

- 5. Pruebe la asignación directa de automontaje con el usuario `contractor1`. Cuando haya terminado, salga de la sesión de usuario `contractor1` en servera.

- 5.1. Despues de que la máquina servera haya terminado de arrancar, inicie sesión en servera con el usuario `student`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

- 5.2. Cambie al usuario `contractor1`.

```
[student@servera ~]$ su - contractor1  
Password: redhat
```

5.3. Enumere el punto de montaje /external.

```
[contractor1@servera ~]$ ls -l /external  
total 4  
-rw-r--r--. 1 root contractors 22 Apr 7 23:34 README.txt
```

5.4. Revise el contenido y pruebe el acceso del punto de montaje /external.

```
[contractor1@servera ~]$ cat /external/README.txt  
###External Folder###  
[contractor1@servera ~]$ echo testing-direct > /external/testing.txt  
[contractor1@servera ~]$ cat /external/testing.txt  
testing-direct
```

5.5. Salga de la sesión de usuario contractor1.

```
[contractor1@servera ~]$ exit  
logout  
[student@servera ~]$
```

► 6. Pruebe la asignación indirecta de automontaje con el usuario operator1. Cuando finalice, cierre sesión de servera.

6.1. Cambie al usuario operator1.

```
[student@servera ~]$ su - operator1  
Password: redhat
```

6.2. Enumere el punto de montaje /internal.

```
[operator1@servera ~]$ ls -l /internal  
total 0
```



nota

Con una asignación indirecta de automontaje, debe acceder a cada subdirectorio exportado para que se monten. En una asignación directa del servicio de automontaje, después de abrir el punto de montaje asignado, podrá ver y acceder inmediatamente a los subdirectorios y al contenido en el directorio exportado.

6.3. Pruebe el acceso a directorio exportado del servicio de montaje automático /internal/west.

```
[operator1@servera ~]$ ls -l /internal/west/  
total 4  
-rw-r--r--. 1 root operators 18 Apr 7 23:34 README.txt
```

capítulo 14 | Acceso al almacenamiento conectado a la red

```
[operator1@servera ~]$ cat /internal/west/README.txt  
###West Folder###  
[operator1@servera ~]$ echo testing-1 > /internal/west/testing-1.txt  
[operator1@servera ~]$ cat /internal/west/testing-1.txt  
testing-1  
[operator1@servera ~]$ ls -l /internal  
total 0  
drwxrws--- 2 root operators 24 Apr 7 23:34 west
```

- 6.4. Pruebe el acceso a directorio exportado del servicio de montaje automático / internal/central.

```
[operator1@servera ~]$ ls -l /internal/central  
total 4  
-rw-r--r-- 1 root operators 21 Apr 7 23:34 README.txt  
[operator1@servera ~]$ cat /internal/central/README.txt  
###Central Folder###  
[operator1@servera ~]$ echo testing-2 > /internal/central/testing-2.txt  
[operator1@servera ~]$ cat /internal/central/testing-2.txt  
testing-2  
[operator1@servera ~]$ ls -l /internal  
total 0  
drwxrws--- 2 root operators 24 Apr 7 23:34 central  
drwxrws--- 2 root operators 24 Apr 7 23:34 west
```

- 6.5. Pruebe el acceso a directorio exportado del servicio de montaje automático / internal/east.

```
[operator1@servera ~]$ ls -l /internal/east  
total 4  
-rw-r--r-- 1 root operators 18 Apr 7 23:34 README.txt  
[operator1@servera ~]$ cat /internal/east/README.txt  
###East Folder###  
[operator1@servera ~]$ echo testing-3 > /internal/east/testing-3.txt  
[operator1@servera ~]$ cat /internal/east/testing-3.txt  
testing-3  
[operator1@servera ~]$ ls -l /internal  
total 0  
drwxrws--- 2 root operators 24 Apr 7 23:34 central  
drwxrws--- 2 root operators 24 Apr 7 23:34 east  
drwxrws--- 2 root operators 24 Apr 7 23:34 west
```

- 6.6. Pruebe el acceso a directorio exportado del servicio de montaje automático / external.

```
[operator1@servera ~]$ ls -l /external  
ls: cannot open directory '/external': Permission denied
```

- 6.7. Regrese a la máquina workstation como el usuario student.

```
[operator1@servera ~]$ exit  
logout  
[student@servera ~]$ exit  
logout  
Connection to servera closed.
```

Finalizar

En la máquina **workstation**, cambie al directorio de inicio de usuario **student** y use el comando **lab** para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish netstorage-autofs
```

Esto concluye la sección.

► Trabajo de laboratorio

Acceso al almacenamiento conectado a la red

Listado de verificación de rendimiento

En este trabajo de laboratorio, configurará el servicio de automontaje con una asignación indirecta, usando exportaciones de un servidor NFSv4.

Resultados

- Instalar los paquetes requeridos para configurar el servicio de automontaje.
- Configurar la asignación indirecta del servicio de automontaje con recursos de un servidor NFSv4 preconfigurado.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este script de inicio determina si los sistemas `servera` y `serverb` son accesibles en la red. El script de inicio configura `serverb` como servidor NFSv4, configura los permisos y exporta los directorios. El script también crea los usuarios y grupos necesarios en los sistemas `servera` y `serverb`.

```
[student@workstation ~]$ lab start netstorage-review
```

Instrucciones

Una empresa de soporte de TI usa un servidor central, `serverb`, para alojar algunos directorios exportados en `/shares` para sus grupos y usuarios. Los usuarios deben ser capaces de iniciar sesión y tener sus directorios exportados montados a pedido y listos para usar, en el directorio `/remote` en `servera`.

Características del entorno:

- La máquina `serverb` comparte el directorio `/shares`, que a su vez contiene los subdirectorios `management`, `production` y `operation`.
- El grupo `managers` está compuesto por los usuarios `manager1` y `manager2`. Tienen acceso de lectura y escritura al directorio exportado `/shares/management`.
- El grupo `production` está compuesto por los usuarios `dbuser1` y `sysadmin1`. Tienen acceso de lectura y escritura al directorio exportado `/shares/production`.
- El grupo `operators` está compuesto por los usuarios `contractor1` y `consultant1`. Tienen acceso de lectura y escritura al directorio exportado `/shares/operation`.
- El punto de montaje principal para `servera` es el directorio `/remote`.
- Use el archivo `/etc/auto.master.d/shares.autofs` como el archivo de asignación maestra y el archivo `/etc/auto.shares` como el archivo de asignación indirecta.

- El directorio exportado /shares/management debe montarse automáticamente en /remote/management en servera.
 - El directorio exportado /shares/production debe montarse automáticamente en /remote/production en servera.
 - El directorio exportado /shares/operation debe montarse automáticamente en /remote/operation en servera.
 - Todas las contraseñas de usuario están definidas en redhat.
1. Inicie sesión en servera e instale los paquetes requeridos.
 2. Configure una asignación indirecta de montaje automático en servera con los recursos exportados de serverb. Cree una asignación indirecta con los archivos denominados /etc/auto.master.d/shares.autofs para la asignación maestra y /etc/auto.shares para el archivo de asignación. Use el directorio /remote como el punto de montaje principal en servera. Reinicie servera para determinar si el servicio autofs se inicia automáticamente.
 3. Pruebe la configuración de autofs con los distintos usuarios. Cuando finalice, cierre sesión de servera.

Evaluación

En la máquina workstation, use el comando lab para confirmar que ha realizado correctamente este ejercicio.

```
[student@workstation ~]$ lab grade netstorage-review
```

Finalizar

En la máquina workstation, cambie al directorio de inicio de usuario student y use el comando lab para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish netstorage-review
```

Esto concluye la sección.

► Solución

Acceso al almacenamiento conectado a la red

Lista de verificación de rendimiento

En este trabajo de laboratorio, configurará el servicio de automontaje con una asignación indirecta, usando exportaciones de un servidor NFSv4.

Resultados

- Instalar los paquetes requeridos para configurar el servicio de automontaje.
- Configurar la asignación indirecta del servicio de automontaje con recursos de un servidor NFSv4 preconfigurado.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este script de inicio determina si los sistemas `servera` y `serverb` son accesibles en la red. El script de inicio configura `serverb` como servidor NFSv4, configura los permisos y exporta los directorios. El script también crea los usuarios y grupos necesarios en los sistemas `servera` y `serverb`.

```
[student@workstation ~]$ lab start netstorage-review
```

Instrucciones

Una empresa de soporte de TI usa un servidor central, `serverb`, para alojar algunos directorios exportados en `/shares` para sus grupos y usuarios. Los usuarios deben ser capaces de iniciar sesión y tener sus directorios exportados montados a pedido y listos para usar, en el directorio `/remote` en `servera`.

Características del entorno:

- La máquina `serverb` comparte el directorio `/shares`, que a su vez contiene los subdirectorios `management`, `production` y `operation`.
- El grupo `managers` está compuesto por los usuarios `manager1` y `manager2`. Tienen acceso de lectura y escritura al directorio exportado `/shares/management`.
- El grupo `production` está compuesto por los usuarios `dbuser1` y `sysadmin1`. Tienen acceso de lectura y escritura al directorio exportado `/shares/production`.
- El grupo `operators` está compuesto por los usuarios `contractor1` y `consultant1`. Tienen acceso de lectura y escritura al directorio exportado `/shares/operation`.
- El punto de montaje principal para `servera` es el directorio `/remote`.
- Use el archivo `/etc/auto.master.d/shares.autofs` como el archivo de asignación maestra y el archivo `/etc/auto.shares` como el archivo de asignación indirecta.

- El directorio exportado /shares/management debe montarse automáticamente en /remote/management en servera.
- El directorio exportado /shares/production debe montarse automáticamente en /remote/production en servera.
- El directorio exportado /shares/operation debe montarse automáticamente en /remote/operation en servera.
- Todas las contraseñas de usuario están definidas en redhat.

1. Inicie sesión en servera e instale los paquetes requeridos.

1.1. Inicie sesión en servera como el usuario student y cambie al usuario root.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

1.2. Instale el paquete autofs.

```
[root@servera ~]# dnf install autofs
...output omitted...
Is this ok [y/N]: y
...output omitted...
Complete!
```

2. Configure una asignación indirecta de montaje automático en servera con los recursos exportados de serverb. Cree una asignación indirecta con los archivos denominados /etc/auto.master.d/shares.autofs para la asignación maestra y /etc/auto.shares para el archivo de asignación. Use el directorio /remote como el punto de montaje principal en servera. Reinicie servera para determinar si el servicio autofs se inicia automáticamente.

2.1. Pruebe el servidor NFS antes de configurar el servicio de automontaje.

```
[root@servera ~]# mount -t nfs serverb.lab.example.com:/shares /mnt
[root@servera ~]# ls -l /mnt
total 0
drwxrwx---. 2 root managers 25 Apr 4 01:13 management
drwxrwx---. 2 root operators 25 Apr 4 01:13 operation
drwxrwx---. 2 root production 25 Apr 4 01:13 production
[root@servera ~]# umount /mnt
```

2.2. Cree un archivo de asignación maestra llamado /etc/auto.master.d/shares.autofs, inserte el siguiente contenido y guarde los cambios.

```
/remote /etc/auto.shares
```

2.3. Cree un archivo de asignación indirecta llamado /etc/auto.shares, inserte el siguiente contenido y guarde los cambios.

```
* -rw, sync, fstype=nfs4 serverb.lab.example.com:/shares/&
```

2.4. Inicie y habilite el servicio `autofs` en `servera`.

```
[root@servera ~]# systemctl enable --now autofs
Created symlink /etc/systemd/system/multi-user.target.wants/autofs.service → /usr/
lib/systemd/system/autofs.service.
```

2.5. Reinicie la máquina `servera`.

```
[root@servera ~]# systemctl reboot
```

3. Pruebe la configuración de `autofs` con los distintos usuarios. Cuando finalice, cierre sesión de `servera`.

3.1. Despues de que la máquina `servera` haya terminado de arrancar, inicie sesión en `servera` con el usuario `student`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

3.2. Cambie al usuario `manager1` y pruebe el acceso.

```
[student@servera ~]$ su - manager1
Password: redhat
[manager1@servera ~]$ ls -l /remote/management/
total 4
-rw-r--r--. 1 root managers 46 Apr  4 01:13 Welcome.txt
[manager1@servera ~]$ cat /remote/management>Welcome.txt
###Welcome to Management Folder on SERVERB###
[manager1@servera ~]$ echo TEST1 > /remote/management/Test.txt
[manager1@servera ~]$ cat /remote/management/Test.txt
TEST1
[manager1@servera ~]$ ls -l /remote/operation/
ls: cannot open directory '/remote/operation/': Permission denied
[manager1@servera ~]$ ls -l /remote/production/
ls: cannot open directory '/remote/production/': Permission denied
[manager1@servera ~]$ exit
logout
[student@servera ~]$
```

3.3. Cambie al usuario `dbuser1` y pruebe el acceso.

```
[student@servera ~]$ su - dbuser1
Password: redhat
[dbuser1@servera ~]$ ls -l /remote/production/
total 4
-rw-r--r--. 1 root production 46 Apr  4 01:13 Welcome.txt
[dbuser1@servera ~]$ cat /remote/production>Welcome.txt
###Welcome to Production Folder on SERVERB###
```

```
[dbuser1@servera ~]$ echo TEST2 > /remote/production/Test.txt
[dbuser1@servera ~]$ cat /remote/production/Test.txt
TEST2
[dbuser1@servera ~]$ ls -l /remote/operation/
ls: cannot open directory '/remote/operation/': Permission denied
[dbuser1@servera ~]$ ls -l /remote/management/
ls: cannot open directory '/remote/management/': Permission denied
[dbuser1@servera ~]$ exit
logout
[student@servera ~]$
```

3.4. Cambie al usuario **contractor1** y pruebe el acceso.

```
[student@servera ~]$ su - contractor1
Password: redhat
[contractor1@servera ~]$ ls -l /remote/operation/
total 4
-rw-r--r--. 1 root operators 45 Apr  4 01:13 Welcome.txt
[contractor1@servera ~]$ cat /remote/operation>Welcome.txt
###Welcome to Operation Folder on SERVERB###
[contractor1@servera ~]$ echo TEST3 > /remote/operation/Test.txt
[contractor1@servera ~]$ cat /remote/operation/Test.txt
TEST3
[contractor1@servera ~]$ ls -l /remote/management/
ls: cannot open directory '/remote/management/': Permission denied
[contractor1@servera ~]$ ls -l /remote/production/
ls: cannot open directory '/remote/production/': Permission denied
[contractor1@servera ~]$ exit
logout
[student@servera ~]$
```

3.5. Explore las opciones de **mount** para la exportación de NFS de automontaje.

```
[student@servera ~]$ mount | grep nfs
rpc_pipefs on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw,relatime)
serverb.lab.example.com:/shares/management on /remote/management type nfs4
(rw,relatime,vers=4.2,rsize=262144,wsize=262144,namlen=255,
sync,proto=tcp,timeo=600,retrans=2,sec=sys,clientaddr=172.25.250.10,
local_lock=none,addr=172.25.250.11)
serverb.lab.example.com:/shares/operation on /remote/operation type nfs4
(rw,relatime,vers=4.2,rsize=262144,wsize=262144,namlen=255,
sync,proto=tcp,timeo=600,retrans=2,sec=sys,clientaddr=172.25.250.10,
local_lock=none,addr=172.25.250.11)
serverb.lab.example.com:/shares/production on /remote/production type nfs4
(rw,relatime,vers=4.2,rsize=262144,wsize=262144,namlen=255,
sync,proto=tcp,timeo=600,retrans=2,sec=sys,clientaddr=172.25.250.10,
local_lock=none,addr=172.25.250.11)
```

3.6. Regrese a la máquina **workstation** como el usuario **student**.

```
[student@servera ~]$ exit
logout
[student@workstation ~]$
```

Evaluación

En la máquina `workstation`, use el comando `lab` para confirmar que ha realizado correctamente este ejercicio.

```
[student@workstation ~]$ lab grade netstorage-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish netstorage-review
```

Esto concluye la sección.

Resumen

- Puede montar y desmontar temporalmente un recurso compartido de NFS desde la línea de comandos.
- Puede montar y desmontar recursos compartidos NFS de forma persistente actualizando el archivo /etc/fstab.
- Puede configurar el servicio `automounter` para montar automáticamente recursos compartidos NFS con mapas directos e indirectos.

capítulo 15

Administración de la seguridad de redes

Meta

Controlar las conexiones de red a los servicios mediante el firewall del sistema.

Objetivos

- Aceptar o rechazar las conexiones de red a los servicios del sistema con reglas de firewalld.

Secciones

- Administración de firewalls del servidor (y ejercicio guiado)

Trabajo de laboratorio

- Administración de la seguridad de redes

Administración de firewalls del servidor

Objetivos

Aceptar o rechazar las conexiones de red a los servicios del sistema con reglas de `firewalld`.

Conceptos de arquitectura del firewall

El kernel de Linux proporciona el marco (framework) `netfilter` para las operaciones de tráfico de red, como el filtrado de paquetes, la traducción de direcciones de red y la traducción de puertos. El marco (framework) `netfilter` incluye *enlaces* para que los módulos del kernel interactúen con los paquetes de red a medida que atraviesan la pila (stack) de red de un sistema. Fundamentalmente, los enlaces `netfilter` son rutinas del kernel que interceptan eventos (por ejemplo, un paquete que ingresa a una interfaz) y ejecutan otras rutinas relacionadas (por ejemplo, reglas de firewall).

El marco (framework) de `nftables`

El marco (framework) de clasificación de paquetes `nftables` se basa en el marco `netfilter` para aplicar reglas de firewall al tráfico de red. En Red Hat Enterprise Linux 9, `nftables` es el núcleo del firewall del sistema y reemplaza al marco (framework) obsoleto `iptables`.

El marco (framework) `nftables` ofrece numerosas ventajas sobre `iptables`, incluida la facilidad de uso y conjuntos de reglas más eficientes. Por ejemplo, el marco (framework) `iptables` requería una regla para cada protocolo, pero las reglas `nftables` se pueden aplicar al tráfico IPv4 e IPv6 simultáneamente. El marco (framework) `iptables` requería el uso de diferentes herramientas, como `iptables`, `ip6tables`, `arptables` y `ebtables`, para cada protocolo, pero el marco `nftables` usa la utilidad de espacio de usuario `nft` para administrar todos los protocolos a través de una única interfaz.



nota

Convierta los archivos de configuración heredados `iptables` en sus equivalentes `nftables` mediante las utilidades `iptables-translate` y `ip6tables-translate`.

El servicio `firewalld`

El servicio `firewalld` es un administrador de firewall dinámico y es el frontend recomendado para el marco (framework) `nftables`. La distribución de Red Hat Enterprise Linux 9 incluye el paquete `firewalld`.

El servicio `firewalld` simplifica la administración de firewall al clasificar todo el tráfico de la red en *zonas*. La zona asignada de un paquete de red depende de criterios como la dirección IP de origen del paquete o la interfaz de red entrante. Cada zona tiene su propia lista de puertos y servicios que están abiertos o cerrados.

**nota**

En el caso de equipos portátiles u otras máquinas que cambian regularmente las redes, el servicio NetworkManager puede configurar automáticamente la zona de firewall para una conexión. Esto es útil en el cambio 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 o corporativas, pero no cuando se conecta a una red inalámbrica pública en la tienda de café local.

El servicio `firewall` verifica la dirección de origen para cada paquete que ingresa al sistema. Si esa dirección de origen está asignada a una zona específica, rigen las reglas de esa zona. Si la dirección de origen no está asignada a una zona, `firewall` asocia el paquete con la zona para la interfaz de red entrante y rigen las reglas para esa zona. Si la interfaz de red no está asociada con una zona, `firewall` envía el paquete con la zona predeterminada.

La zona predeterminada no es una zona separada, sino una designación asignada a una zona existente. Inicialmente, el servicio `firewall` designa la zona `public` como la zona predeterminada y asigna la interfaz de bucle invertido `lo` a la zona `trusted`.

La mayoría de las zonas permiten el tráfico a través del firewall que relaciona una lista de puertos y protocolos particulares (como `631/udp`) o una configuración de servicios predefinidos (como `ssh`). Normalmente, si el tráfico no relaciona un puerto y protocolo o servicio permitidos, entonces se rechaza. La zona `trusted`, que permite todo el tráfico de forma predeterminada, es una excepción.

Zonas predefinidas

El servicio `firewall` usa zonas predefinidas, que puede personalizar. De forma predeterminada, todas las zonas permiten todo el tráfico entrante que sea parte de una sesión iniciada existente por el sistema y también todo el tráfico saliente. En la siguiente tabla, se detalla la configuración de zona inicial.

Configuración predeterminada de zonas `firewall`

Nombre de la zona	Configuración predeterminada
<code>trusted</code>	Permite todo el tráfico entrante.
<code>home</code>	Rechaza el tráfico entrante, a menos que esté relacionado con tráfico saliente o que relacione los servicios predefinidos <code>ssh</code> , <code>mdns</code> , <code>ipp-client</code> , <code>samba-client</code> o <code>dhcpv6-client</code> .
<code>internal</code>	Rechaza el tráfico entrante, a menos que esté relacionado con tráfico saliente o que relacione los servicios predefinidos <code>ssh</code> , <code>mdns</code> , <code>ipp-client</code> , <code>samba-client</code> o <code>dhcpv6-client</code> (lo mismo que la zona <code>home</code> para empezar).
<code>work</code>	Rechaza el tráfico entrante, a menos que esté relacionado con tráfico saliente o que relacione los servicios predefinidos <code>ssh</code> , <code>ipp-client</code> o <code>dhcpv6-client</code> .

Nombre de la zona	Configuración predeterminada
public	Rechaza el tráfico entrante, a menos que esté relacionado con tráfico saliente o que relacione los servicios predefinidos ssh o dhcipv6-client. La zona predeterminada para interfaces de red recientemente agregadas.
external	Rechaza el tráfico entrante a menos que esté relacionado con tráfico saliente o que relacione el servicio predefinido ssh. El tráfico IPv4 saliente reenviado a través de esta zona es enmascarado para que luzca como si se hubiera originado desde la dirección IPv4 de la interfaz de red saliente.
dmz	Rechaza el tráfico entrante a menos que esté relacionado con tráfico saliente o que relacione el servicio predefinido ssh.
block	Rechaza todo el tráfico entrante, a menos que esté relacionado con tráfico saliente.
drop	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 las zonas predefinidas y sus usos previstos, consulte la página del manual `firewalld.zones(5)`.

Servicios predefinidos

El servicio `firewallld` incluye una serie de configuraciones predefinidas para servicios comunes, para simplificar la configuración de reglas de firewall. Por ejemplo, en lugar de investigar los puertos relevantes para un servidor NFS, use la configuración predefinida `nfs` para crear reglas para los puertos y protocolos correctos. En la siguiente tabla, se enumeran las configuraciones de servicio predefinidas que el servicio `firewallld` usa en su configuración predeterminada.

Servicios `firewallld` predefinidos seleccionados

Nombre del servicio	Configuración
ssh	Servidor SSH local. Tráfico a 22/tcp.
dhcipv6-client	Cliente DHCPv6 local. Tráfico a 546/udp en la red fe80::/64 IPv6.
ipp-client	Impresión IPP local. Tráfico a 631/udp.
samba-client	Archivo Windows local y cliente de intercambio de impresión. Tráfico a 137/udp y 138/udp.
mdns	Resolución del nombre del enlace local DNS (mDNS) multidifusión (multicast). Tráfico a 5353/udp a las direcciones de multidifusión (multicast) 224.0.0.251 (IPv4) o ff02::fb (IPv6).

El paquete `firewallld` incluye muchas configuraciones de servicio predefinidas. Puede enumerar los servicios con el comando `firewall-cmd --get-services`.

```
[root@host ~]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule amanda-client amanda-k5-client amqp amqps
apcupsd audit bacula bacula-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet
bitcoin-testnet-rpc bittorrent-lsd ceph ceph-mon cfengine cockpit collectd
...output omitted...
```

Si las configuraciones de servicio predefinidas no son adecuadas para su escenario, puede especificar manualmente los puertos y protocolos requeridos. Puede usar la interfaz gráfica de la consola web para revisar los servicios predefinidos y para definir manualmente puertos y protocolos adicionales.

Configuración del daemon firewalld

Entre otras, estas son dos formas comunes que usan los administradores de sistemas para interactuar con el servicio `firewalld`:

- La interfaz gráfica de la consola web
- La herramienta de línea de comandos `firewall-cmd`

Configuración de los servicios de firewall con la consola web

Para administrar los servicios de firewall con la consola web, debe iniciar sesión y aumentar los privilegios. Puede aumentar los privilegios haciendo clic en los botones **Limited access** (Acceso limitado) o **Turn on administrative access** (Activar acceso administrativo). A continuación, ingrese su contraseña cuando se le solicite. El modo administrativo eleva los privilegios en función de la configuración de sudo del usuario. Como recordatorio de seguridad, recuerde que debe volver al modo de acceso limitado una vez que realice en su sistema la tarea que requiere privilegios administrativos.

Haga clic en la opción **Networking (Redes)** en el menú de navegación izquierdo para mostrar la sección **Firewall (Firewall)** en la página principal de redes. Haga clic en las zonas del botón **Edit rules and zones** (Editar reglas y zonas) para navegar a la página **Firewall (Firewall)**.

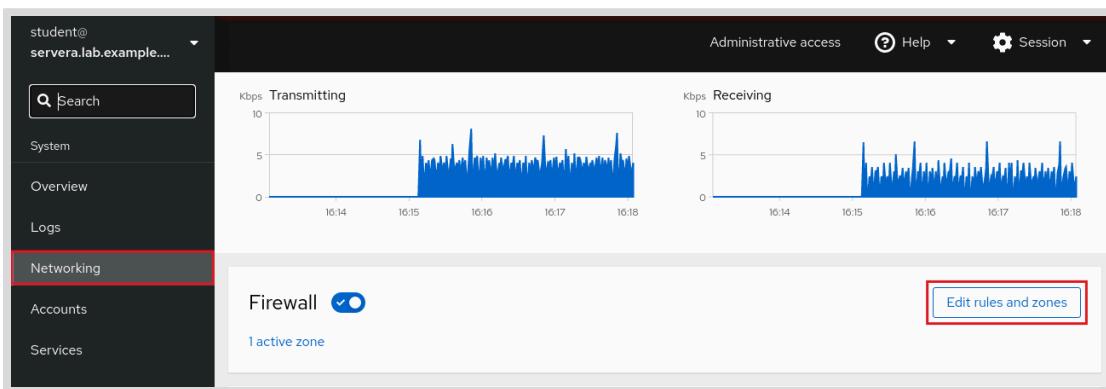


Figura 15.1: Páginas de redes de la consola web

La página **Firewall (Firewall)** muestra las zonas activas y sus servicios permitidos. Haga clic en el botón de la flecha (>) a la izquierda del nombre del servicio para ver los detalles del servicio. Para agregar un servicio a una zona, haga clic en el botón **Add services** (Aregar servicios) en la esquina superior derecha de la zona correspondiente.

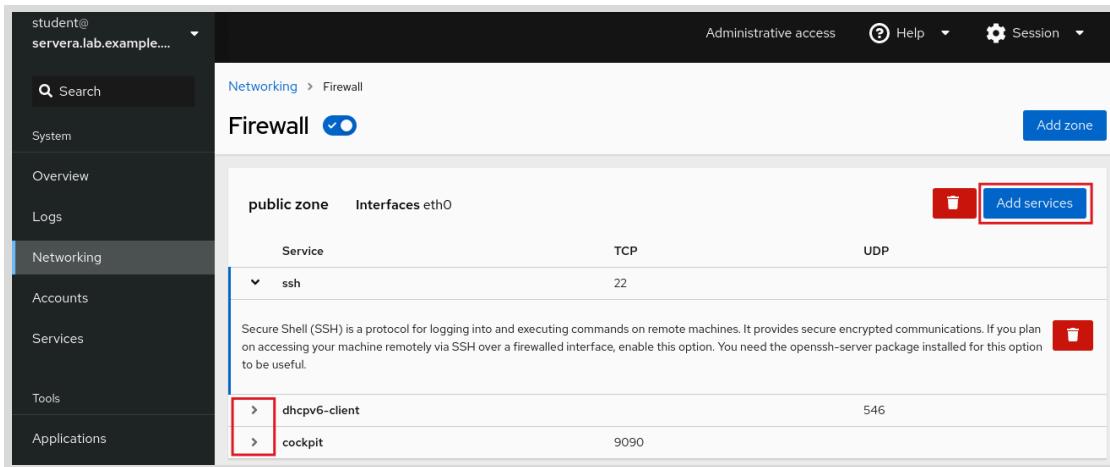


Figura 15.2: Página de firewall de la consola web

La página Add Services (Agregar servicios) muestra los servicios predefinidos disponibles.

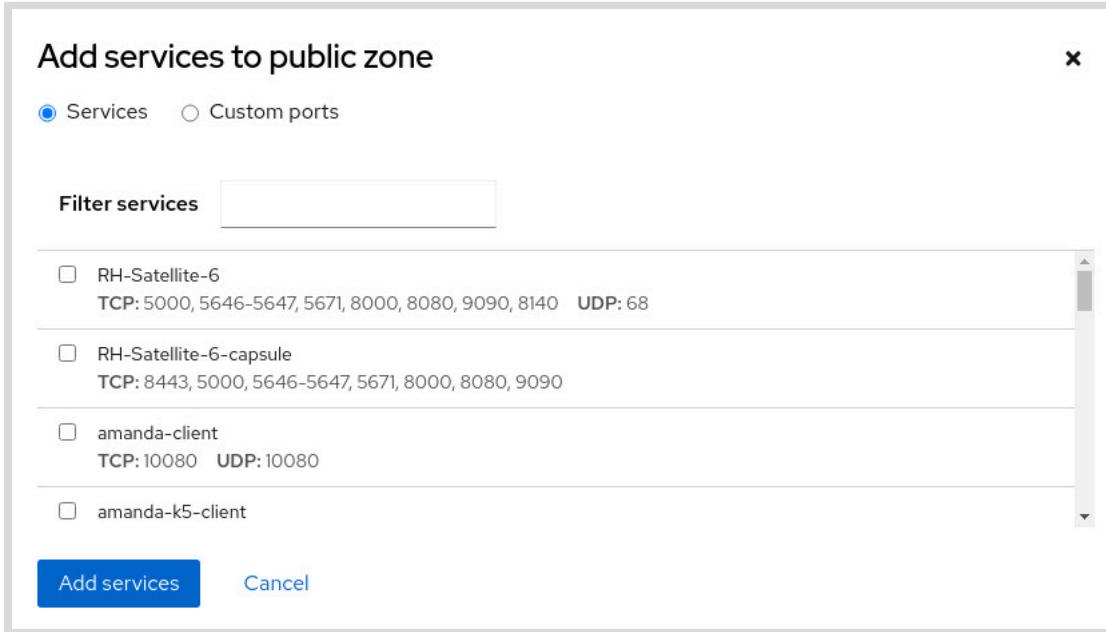


Figura 15.3: Menú para agregar servicios en la consola web

Para seleccionar un servicio, desplácese por la lista o seleccione una opción en el cuadro de texto **Filter services** (Filtrar servicios). En el siguiente ejemplo, la cadena `http` filtra las opciones a servicios relacionados con la web. Seleccione la casilla de verificación a la izquierda del servicio para que el firewall los permita. Haga clic en el botón **Add services** (Agregar servicios) para completar el proceso.

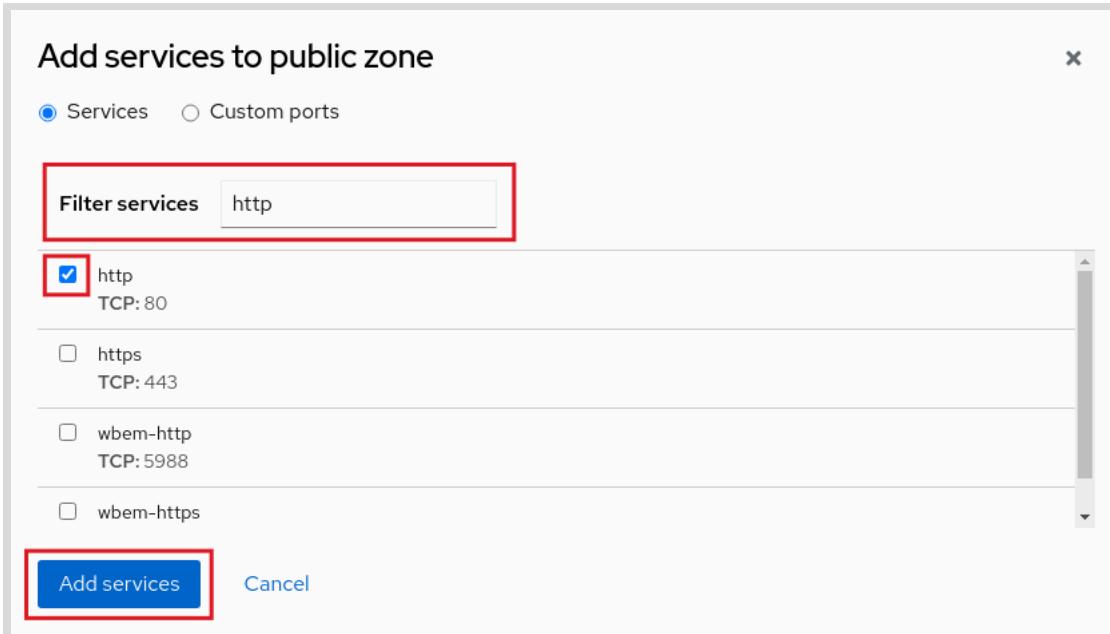


Figura 15.4: Opciones de menú para agregar servicios en la consola web

La interfaz vuelve a la página de Firewall (Firewall), donde puede revisar la lista actualizada de servicios permitidos.

The screenshot shows the 'Networking > Firewall' page. On the left is a sidebar with 'Networking' selected. The main area shows a table for the 'public zone' on 'Interfaces eth0'. The table includes columns for 'Service', 'TCP', and 'UDP'. It lists several services: ssh (port 22), dhcpcv6-client (port 546), cockpit (port 9090), and http (port 80). At the bottom right of the table is a 'Delete' icon and a 'Add services' button, both of which are highlighted with red boxes.

Figura 15.5: Descripción general del firewall de la consola web

Configuración de firewall desde la línea de comandos

El comando `firewall-cmd` interactúa con el daemon `firewalld`. Se instala como parte del paquete `firewalld` y está disponible para los administradores que prefieren trabajar en la línea de comandos a los fines de trabajar en sistemas sin un entorno gráfico o ejecutar el scripting de la configuración de firewall.

En la siguiente tabla, se detallan comandos de `firewall-cmd` usados frecuentemente, junto con una explicación. Observe que, a menos que se especifique lo contrario, casi todos los comandos funcionan en la configuración de *tiempo de ejecución*, a menos que se especifique la opción `--permanent`. Si se especifica la opción `--permanent`, debe activar la configuración ejecutando también el comando `firewall-cmd --reload`, que lee la configuración permanente actual y la aplica como la nueva configuración de tiempo de ejecución. Muchos de los comandos detallados toman la opción `--zone=ZONE` para determinar qué zona afectan. Cuando se requiera una máscara de red, use la notación CIDR (como 192.168.1/24).

Comandos firewall-cmd	Explicación
--get-default-zone	Consultar la zona predeterminada actual.
--set-default-zone=ZONE	Configurar la zona predeterminada. Esto cambia tanto la configuración del tiempo de ejecución como la permanente.
--get-zones	Mostrar todas las zonas disponibles.
--get-active-zones	Mostrar todas las zonas que están actualmente en uso (tienen una interfaz u origen conectados a esta), junto con la información de su interfaz y origen.
--add-source=CIDR [--zone=ZONE]	Enrutar todo el tráfico que proviene de la dirección IP o red/máscara de red a la zona especificada. Si no se proporciona ninguna opción --zone=, se usa la zona predeterminada.
--remove-source=CIDR [--zone=ZONE]	Eliminar la regla que enruta todo el tráfico que proviene de la red de la dirección IP o red. Si no se proporciona ninguna opción --zone=, se usa la zona predeterminada.
--add-interface=INTERFACE [--zone=ZONE]	Enrutar todo el tráfico que proviene de <i>INTERFACE</i> a la zona especificada. Si no se proporciona ninguna opción --zone=, se usa la zona predeterminada.
--change-interface=INTERFACE [--zone=ZONE]	Asociar la interfaz con ZONE en lugar de su zona actual. Si no se proporciona ninguna opción --zone=, se usa la zona predeterminada.
--list-all [--zone=ZONE]	Detallar todas las interfaces, fuentes, servicios y puertos configurados para ZONE. Si no se proporciona ninguna opción --zone=, se usa la zona predeterminada.
--list-all-zones	Recuperar toda la información para todas las zonas (interfaces, fuentes, puertos, servicios).
--add-service=SERVICE [--zone=ZONE]	Permitir el tráfico a SERVICE. Si no se proporciona ninguna opción --zone=, se usa la zona predeterminada.
--add-port=PORT/PROTOCOL [--zone=ZONE]	Permitir el tráfico a los puertos PORT/PROTOCOL. Si no se proporciona ninguna opción --zone=, se usa la zona predeterminada.

Comandos firewall-cmd	Explicación
--remove-service=SERVICE [--zone=ZONE]	Elimina <i>SERVICE</i> de la lista permitida para la zona. Si no se proporciona ninguna opción --zone=, se usa la zona predeterminada.
--remove-port=PORT/PROTOCOL [--zone=ZONE]	Eliminar los puertos <i>PORT/PROTOCOL</i> de la lista permitida para la zona. Si no se proporciona ninguna opción --zone=, se usa la zona predeterminada.
--reload	Dejar caer la configuración del tiempo de ejecución y aplicar la configuración persistente.

El siguiente ejemplo configura la zona predeterminada para `dmz`, asigna todo el tráfico proveniente de la red `192.168.0.0/24` a la zona `internal` y abren los puertos de red para el servicio `mysql` en la zona `internal`.

```
[root@host ~]# firewall-cmd --set-default-zone=dmz
[root@host ~]# firewall-cmd --permanent --zone=internal \
--add-source=192.168.0.0/24
[root@host ~]# firewall-cmd --permanent --zone=internal --add-service=mysql
[root@host ~]# firewall-cmd --reload
```



nota

En situaciones donde la sintaxis básica no es suficiente, puede agregar *reglas enriquecidas* para escribir reglas complejas. Si aun así la sintaxis de las reglas enriquecidas no es suficiente, también puede usar reglas de Configuración directa (sintaxis de `nft` sin formato mezclada con las reglas de `firewalld`). Esta configuración avanzada no está incluida en el alcance de este capítulo.



Referencias

Páginas del manual: `firewall-cmd(1)`, `firewalld(1)`, `firewalld.zone(5)`, `firewalld.zones(5)` y `nft(8)`

► Ejercicio Guiado

Administración de firewalls del servidor

En este ejercicio, controla el acceso a los servicios del sistema mediante el ajuste de las reglas del firewall del sistema con `firewalld`.

Resultados

- Configurar reglas de firewall para controlar el acceso a los servicios.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start netsecurity-firewalls
```

Instrucciones

- 1. Inicie sesión en la máquina `servera` como el usuario `student` y cambie al usuario `root`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

- 2. Instale los paquetes `httpd` y `mod_ssl`. Estos paquetes proporcionan el servidor web Apache y las extensiones necesarias para que el servidor web sirva contenido mediante SSL.

```
[root@servera ~]# dnf install httpd mod_ssl
...output omitted...
Is this ok [y/N]: y
...output omitted...
Complete!
```

- 3. Cree el archivo `/var/www/html/index.html`. Agregue la siguiente línea de texto: `I am servera..`

```
[root@servera ~]# echo 'I am servera.' > /var/www/html/index.html
```

- 4. Inicie y habilite el servicio `httpd`.

```
[root@servera ~]# systemctl enable --now httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/
lib/systemd/system/httpd.service.
```

- 5. Regrese a la máquina **workstation** como el usuario **student**.

```
[root@servera ~]# exit
logout
[student@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$
```

- 6. Desde **workstation**, intente acceder al servidor web en **servera** por medio del puerto no cifrado 80/TCP y del puerto encapsulado SSL 443/TCP. Ambos intentos deberían fallar.

- 6.1. El comando **curl** fallará.

```
[student@workstation ~]$ curl http://servera.lab.example.com
curl: (7) Failed to connect to servera.lab.example.com port 80: No route to host
```

- 6.2. El comando **curl** con la opción **-k** para conexiones inseguras también fallará.

```
[student@workstation ~]$ curl -k https://servera.lab.example.com
curl: (7) Failed to connect to servera.lab.example.com port 443: No route to host
```

- 7. Verifique que el servicio **firewalld** en **servera** esté habilitado y en ejecución.

```
[student@workstation ~]$ ssh student@servera 'systemctl status firewalld'
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor
   preset: enabled)
     Active: active (running) since Wed 2022-04-13 11:22:50 EDT; 7min ago
       Docs: man:firewalld(1)
   Main PID: 768 (firewalld)
     Tasks: 2 (limit: 10798)
    Memory: 39.9M
      CPU: 584ms
     CGroup: /system.slice/firewalld.service
             └─768 /usr/bin/python3 -s /usr/sbin/firewalld --nofork --nopid

Apr 13 11:22:49 servera.lab.example.com systemd[1]: Starting firewalld - dynamic
firewall daemon...
Apr 13 11:22:50 servera.lab.example.com systemd[1]: Started firewalld - dynamic
firewall daemon.
```

- 8. Desde **workstation**, abra Firefox e inicie sesión en la consola web que se ejecuta en **servera** para agregar el servicio **https** a la zona de **firewall public**.

- 8.1. Abra Firefox y navegue hasta `https://servera.lab.example.com:9090` para acceder a la consola web. Haga clic en **Advanced** (Avanzado) y **Accept the Risk and Continue** (Aceptar el riesgo y continuar) para aceptar el certificado autofirmado.
 - 8.2. Inicie sesión con el usuario **student** y proporcione **student** como contraseña.
 - 8.3. Haga clic en **Turn on administrative access** (Aceptar el riesgo y continuar) e ingrese la contraseña **student** nuevamente.
 - 8.4. Haga clic en **Networking** (Redes) en la barra de navegación izquierda.
 - 8.5. Haga clic en **Edit rules and zones** (Editar reglas y zonas) en la sección **Firewall** (Firewall) de la página **Networking** (Redes).
 - 8.6. Haga clic en **Add services** (Agregar servicios) ubicado en la esquina superior derecha de la sección **public zone** (zona pública).
 - 8.7. En la interfaz **Add services** (Agregar servicios), desplácese hacia abajo o use **Filter services** (Filtrar servicios) para ubicar y seleccionar la casilla de verificación junto al servicio **https**.
 - 8.8. Haga clic en **Add services** (Agregar servicios) para aplicar el cambio.
- 9. Regrese a un terminal en **workstation** y verifique su trabajo intentando acceder al contenido del servidor web de **servera**.

- 9.1. El comando `curl` para el puerto estándar 80 debe fallar.

```
[student@workstation ~]$ curl http://servera.lab.example.com
curl: (7) Failed to connect to servera.lab.example.com port 80: No route to host
```

- 9.2. El comando `curl` con la opción `-k` en el puerto 443 debería funcionar correctamente.

```
[student@workstation ~]$ curl -k https://servera.lab.example.com
I am servera.
```

Finalizar

En la máquina **workstation**, cambie al directorio de inicio de usuario **student** y use el comando **lab** para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish netsecurity-firewalls
```

Esto concluye la sección.

► Trabajo de laboratorio

Administración de la seguridad de redes

En este trabajo de laboratorio, configurará un firewall y los ajustes de SELinux para permitir el acceso a múltiples servidores web que se ejecutan en el mismo host.

Resultados

- Configurar el firewall y los ajustes de SELinux en un host del servidor web.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start netsecurity-review
```

Instrucciones

Su empresa ha decidido ejecutar una nueva aplicación web. Esta aplicación escucha en puertos 80/TCP y 1001/TCP. También debe poner a disposición el puerto 22/TCP para el acceso ssh. Todos los cambios que hace deben persistir en un reinicio.



Importante

El entorno de aprendizaje en línea de Red Hat necesita el puerto 5900/TCP para permanecer disponible para usar la interfaz gráfica. Este puerto también es conocido en el servicio `vnc-server`. Si accidentalmente se bloquea a usted mismo fuera de la máquina `serverb`, puede intentar recuperar el acceso al usar el comando `ssh` para su máquina `serverb` desde su máquina `workstation` o restablecer su máquina `serverb`. Si elige restablecer su máquina `serverb`, debe 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.

- Desde la máquina `workstation`, pruebe acceder al servidor web predeterminado en `http://serverb.lab.example.com` y al host virtual en `http://serverb.lab.example.com:1001`.
- Inicie sesión en la máquina `serverb` para determinar qué está impidiendo el acceso a los servidores web.
- Configure SELinux para que permita que el servicio `httpd` escuche en el puerto 1001/TCP.
- Desde `workstation`, pruebe acceder nuevamente al servidor web predeterminado en `http://serverb.lab.example.com` y al host virtual en `http://serverb.lab.example.com:1001`.
- Inicie sesión en la máquina `serverb` para determinar si los puertos correctos están asignados al firewall.

6. Agregue el puerto 1001/TCP a la configuración permanente para la zona de red public (pública). Confirme su configuración.
7. Desde `workstation`, confirme que el servidor web predeterminado en `serverb.lab.example.com` vuelva a SERVER B y que el host virtual en `serverb.lab.example.com:1001` vuelva a VHOST 1.

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade netsecurity-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish netsecurity-review
```

Esto concluye la sección.

► Solución

Administración de la seguridad de redes

En este trabajo de laboratorio, configurará un firewall y los ajustes de SELinux para permitir el acceso a múltiples servidores web que se ejecutan en el mismo host.

Resultados

- Configurar el firewall y los ajustes de SELinux en un host del servidor web.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start netsecurity-review
```

Instrucciones

Su empresa ha decidido ejecutar una nueva aplicación web. Esta aplicación escucha en puertos 80/TCP y 1001/TCP. También debe poner a disposición el puerto 22/TCP para el acceso ssh. Todos los cambios que hace deben persistir en un reinicio.



Importante

El entorno de aprendizaje en línea de Red Hat necesita el puerto 5900/TCP para permanecer disponible para usar la interfaz gráfica. Este puerto también es conocido en el servicio `vnc-server`. Si accidentalmente se bloquea a usted mismo fuera de la máquina `serverb`, puede intentar recuperar el acceso al usar el comando `ssh` para su máquina `serverb` desde su máquina `workstation` o restablecer su máquina `serverb`. Si elige restablecer su máquina `serverb`, debe 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.

- Desde la máquina `workstation`, pruebe acceder al servidor web predeterminado en `http://serverb.lab.example.com` y al host virtual en `http://serverb.lab.example.com:1001`.
 - Pruebe acceder al servidor web en `http://serverb.lab.example.com`. La prueba falla actualmente. El servidor web debería volver a SERVER B.

```
[student@workstation ~]$ curl http://serverb.lab.example.com
curl: (7) Failed to connect to serverb.lab.example.com port 80: Connection refused
```

- Pruebe acceder al host virtual en `http://serverb.lab.example.com:1001`. La prueba falla actualmente. Por último, el host virtual debería volver a VHOST 1.

```
[student@workstation ~]$ curl http://serverb.lab.example.com:1001
curl: (7) Failed to connect to serverb.lab.example.com port 1001: No route to host
```

2. Inicie sesión en la máquina `serverb` para determinar qué está impidiendo el acceso a los servidores web.

- 2.1. Inicie sesión en la máquina `serverb` con el usuario `student`.

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
[student@serverb ~]$
```

- 2.2. Determine si el servicio `httpd` está activo.

```
[student@serverb ~]$ systemctl is-active httpd
inactive
```

- 2.3. Habilite e inicie el servicio `httpd`. El servicio `httpd` no puede iniciarse.

```
[student@serverb ~]$ sudo systemctl enable --now httpd
[sudo] password for student: student
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/
lib/systemd/system/httpd.service.
Job for httpd.service failed because the control process exited with error code.
See "systemctl status httpd.service" and "journalctl -xeu httpd.service" for
details.
```

- 2.4. Investigue los motivos que el servicio `httpd` no se pudo iniciar.

```
[student@serverb ~]$ systemctl status httpd.service
× httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor
   preset: disabled)
     Active: failed (Result: exit-code) since Wed 2022-04-13 06:55:01 EDT; 2min
      52s ago
       Docs: man:httpd.service(8)
      Process: 1640 ExecStart=/usr/sbin/httpd $OPTIONS -DFOREGROUND (code=exited,
      status=1/FAILURE)
     Main PID: 1640 (code=exited, status=1/FAILURE)
       Status: "Reading configuration..."
        CPU: 31ms

Apr 13 06:55:01 serverb.lab.example.com systemd[1]: Starting The Apache HTTP
Server...
Apr 13 06:55:01 serverb.lab.example.com httpd[1640]: (13)Permission denied:
AH00072: make_sock: could not bind to address [::]:1001
Apr 13 06:55:01 serverb.lab.example.com httpd[1640]: (13)Permission denied:
AH00072: make_sock: could not bind to address 0.0.0.0:1001
Apr 13 06:55:01 serverb.lab.example.com httpd[1640]: no listening sockets
available, shutting down
Apr 13 06:55:01 serverb.lab.example.com httpd[1640]: AH00015: Unable to open logs
```

```
Apr 13 06:55:01 serverb.lab.example.com systemd[1]: httpd.service: Main process exited, code=exited, status=1/FAILURE
Apr 13 06:55:01 serverb.lab.example.com systemd[1]: httpd.service: Failed with result 'exit-code'.
Apr 13 06:55:01 serverb.lab.example.com systemd[1]: Failed to start The Apache HTTP Server.
```

- 2.5. Compruebe si SELinux está impidiendo que el servicio `httpd` haga referencia al puerto 1001/TCP.

```
[student@serverb ~]$ sudo sealert -a /var/log/audit/audit.log
100% done
found 1 alerts in /var/log/audit/audit.log
-----
SELinux is preventing /usr/sbin/httpd from name_bind access on the tcp_socket port 1001.

***** Plugin bind_ports (99.5 confidence) suggests *****

If you want to allow /usr/sbin/httpd to bind to network port 1001
Then you need to modify the port type.
Do
# semanage port -a -t PORT_TYPE -p tcp 1001
    where PORT_TYPE is one of the following: http_cache_port_t, http_port_t,
    jboss_management_port_t, jboss.messaging_port_t, ntop_port_t, puppet_port_t.

***** Plugin catchall (1.49 confidence) suggests *****

...output omitted...
```

3. Configure SELinux para que permita que el servicio `httpd` escuche en el puerto 1001/TCP.

- 3.1. Use el comando `semanage` para encontrar el tipo de puerto correcto.

```
[student@serverb ~]$ sudo semanage port -l | grep 'http'
http_cache_port_t          tcp      8080, 8118, 8123, 10001-10010
http_cache_port_t          udp      3130
http_port_t                 tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t         tcp      5988
pegasus_https_port_t        tcp      5989
```

- 3.2. Vincule el puerto 1001/TCP al tipo `http_port_t`.

```
[student@serverb ~]$ sudo semanage port -a -t http_port_t -p tcp 1001
```

- 3.3. Confirme si ese puerto 1001/TCP está enlazado con el tipo de puerto `http_port_t`.

```
[student@serverb ~]$ sudo semanage port -l | grep '^http_port_t'
http_port_t                 tcp      1001, 80, 81, 443, 488, 8008, 8009, 8443, 9000
```

- 3.4. Habilite e inicie el servicio `httpd`.

```
[student@serverb ~]$ sudo systemctl enable --now httpd
```

- 3.5. Verifique si el servicio httpd está en ejecución.

```
[student@serverb ~]$ systemctl is-active httpd
active
[student@serverb ~]$ systemctl is-enabled httpd
enabled
```

- 3.6. Regrese a la máquina workstation como el usuario student.

```
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@workstation ~]$
```

4. Desde workstation, pruebe acceder nuevamente al servidor web predeterminado en `http://serverb.lab.example.com` y al host virtual en `http://serverb.lab.example.com:1001`.

- 4.1. Pruebe acceder al servidor web en `http://serverb.lab.example.com`. El servidor web debería volver a SERVER B.

```
[student@workstation ~]$ curl http://serverb.lab.example.com
SERVER B
```

- 4.2. Pruebe acceder al host virtual en `http://serverb.lab.example.com:1001`. La prueba sigue fallando.

```
[student@workstation ~]$ curl http://serverb.lab.example.com:1001
curl: (7) Failed to connect to serverb.lab.example.com port 1001: No route to host
```

5. Inicie sesión en la máquina serverb para determinar si los puertos correctos están asignados al firewall.

- 5.1. Inicie sesión en la máquina serverb como el usuario student.

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
[student@serverb ~]$
```

- 5.2. Verifique que la zona de firewall predeterminada esté configurada en la zona public.

```
[student@serverb ~]$ firewall-cmd --get-default-zone
public
```

- 5.3. Si el paso anterior no establece la zona public como la zona predeterminada, corríjala con el siguiente comando:

```
[student@serverb ~]$ sudo firewall-cmd --set-default-zone public
```

- 5.4. Determine los puertos abiertos listados en la zona de red public.

```
[student@serverb ~]$ sudo firewall-cmd --permanent --zone=public --list-all
[sudo] password for student: student
public
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
    services: cockpit dhcpv6-client http ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

6. Agregue el puerto 1001/TCP a la configuración permanente para la zona de red public (pública). Confirme su configuración.

- 6.1. Agregue el puerto 1001/TCP a la zona de red public (pública).

```
[student@serverb ~]$ sudo firewall-cmd --permanent --zone=public \
--add-port=1001/tcp
success
```

- 6.2. Vuelva a cargar la configuración del firewall.

```
[student@serverb ~]$ sudo firewall-cmd --reload
success
```

- 6.3. Verifique su configuración.

```
[student@serverb ~]$ sudo firewall-cmd --permanent --zone=public --list-all
public
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
    services: cockpit dhcpv6-client http ssh
  ports: 1001/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

- 6.4. Regrese a la máquina workstation como el usuario student.

```
[student@serverb ~]$ exit  
logout  
Connection to serverb closed.  
[student@workstation ~]$
```

7. Desde `workstation`, confirme que el servidor web predeterminado en `serverb.lab.example.com` vuelva a SERVER B y que el host virtual en `serverb.lab.example.com:1001` vuelva a VHOST 1.

7.1. Pruebe acceder al servidor web en `http://serverb.lab.example.com`.

```
[student@workstation ~]$ curl http://serverb.lab.example.com  
SERVER B
```

7.2. Pruebe acceder al host virtual en `http://serverb.lab.example.com:1001`.

```
[student@workstation ~]$ curl http://serverb.lab.example.com:1001  
VHOST 1
```

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade netsecurity-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish netsecurity-review
```

Esto concluye la sección.

Resumen

- El marco (framework) **netfilter** permite a los módulos del kernel inspeccionar cada paquete que atraviesa el sistema, incluidos todos los paquetes de red entrantes, salientes o reenviados.
- El servicio **firewalld** simplifica la administración al clasificar todo el tráfico de la red en zonas. Cada zona tiene su propia lista de puertos y servicios. La zona **public** (pública) se establece como la zona predeterminada.
- El servicio **firewalld** incluye diversos servicios predefinidos. Puede enumerarlos con el comando **firewall-cmd --get-services**.

capítulo 16

Ejecución de contenedores

Meta

Obtener, ejecutar y administrar servicios livianos simples como contenedores en un único servidor de Red Hat Enterprise Linux.

Objetivos

- Explicar los conceptos de contenedores y las tecnologías centrales (core) para crear, almacenar y ejecutar contenedores.
- Analizar las herramientas de administración de contenedores para usar registros para almacenar y recuperar imágenes, y para implementar, consultar y acceder a contenedores.
- Proporcionar almacenamiento persistente para los datos del contenedor al compartir el almacenamiento desde el host del contenedor y configurar una red de contenedores.
- Configurar un contenedor como servicio `systemd` y configurar un servicio de contenedor para que se inicie en el momento del arranque.

Secciones

- Conceptos de contenedores (y cuestionario)
- Implementación de contenedores (y ejercicio guiado)
- Administración del almacenamiento de contenedores y los recursos de red (y ejercicio guiado)
- Administración de contenedores como servicios de sistemas (y ejercicio guiado)

Trabajo de laboratorio

Ejecución de contenedores

Conceptos de contenedores

Objetivos

Explicar los conceptos de contenedores y las tecnologías centrales (core) para crear, almacenar y ejecutar contenedores.

Tecnología de contenedores

Por lo general, las aplicaciones de software dependen de otras librerías, archivos de configuración o servicios proporcionados por el entorno de tiempo de ejecución. En general, el entorno de tiempo de ejecución para una aplicación de software se instala en un sistema operativo que se ejecuta en un host físico o una máquina virtual. A continuación, los administradores instalan las dependencias de la aplicación en la parte superior del sistema operativo.

En Red Hat Enterprise Linux, los sistemas de paquetes como RPM se usan para ayudar a administrar las dependencias de las aplicaciones. Cuando instala el paquete `httpd`, el sistema RPM garantiza que también se instalen las librerías y las demás dependencias correspondientes para ese paquete.

El principal inconveniente de las aplicaciones de software implementadas tradicionalmente es que estas dependencias están entremezcladas con el entorno de tiempo de ejecución. Una aplicación puede necesitar versiones de software anteriores o posteriores al software provisto con el sistema operativo. De manera similar, dos aplicaciones en el mismo sistema pueden requerir versiones diferentes e incompatibles del mismo software.

Una forma de resolver estos conflictos es empaquetar e implementar la aplicación como un *contenedor*. Un contenedor es un conjunto de uno o más procesos que están aislados del resto del sistema. Los contenedores de software proporcionan una forma de empaquetar aplicaciones y simplificar la implementación y la administración.

Piense en un contenedor de transporte físico. Un contenedor de envío es una forma estándar de empaquetar y enviar mercancías. Se etiqueta, se carga, se descarga y se transporta de una ubicación a otra como si se tratase de una sola caja. El contenido del contenedor se aísla del contenido de otros contenedores para que no se afecten unos a otros. Estos principios subyacentes también se aplican a los contenedores de software.

Red Hat Enterprise Linux soporta contenedores mediante el uso de las siguientes tecnologías centrales (core):

- *Grupos de control (cgroups)* para administrar recursos.
- *Espacios de nombres (Namespaces)* para aislar procesos.
- SELinux y Seccomp (modo de computación segura) para aplicar (enforce) límites de seguridad.



nota

Para obtener un análisis más exhaustivo de la arquitectura y seguridad del contenedor, consulte el informe técnico "Diez capas de seguridad de contenedores" [<https://www.redhat.com/en/resources/container-security-openshift-cloud-devops-whitepaper>].

Diferencias entre contenedores y máquinas virtuales

Los contenedores ofrecen muchos de los mismos beneficios que las máquinas virtuales, como seguridad, almacenamiento y aislamiento de redes.

Ambas tecnologías aíslan las librerías de aplicaciones y los recursos de tiempo de ejecución del sistema operativo del host o del hipervisor y viceversa.

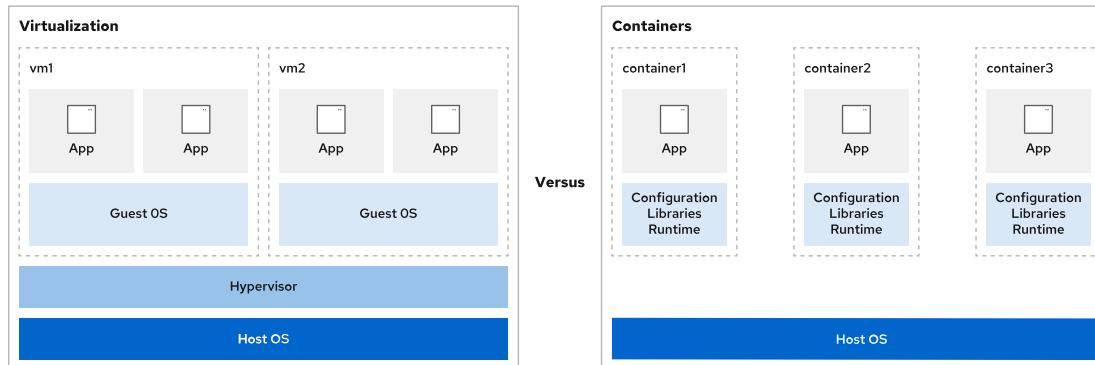


Figura 16.1: Comparación entre virtualización y contenerización

Los contenedores y las máquinas virtuales interactúan de manera diferente con el hardware y el sistema operativo subyacente.

Una máquina virtual tiene las siguientes características:

- Permite que varios sistemas operativos se ejecuten simultáneamente en una única plataforma de hardware.
- Usa un hipervisor para dividir el hardware en varios sistemas de hardware virtuales.
- Requiere un entorno de sistema operativo completo para dar soporte a la aplicación.

Un contenedor tiene las siguientes características:

- Se ejecuta directamente en el sistema operativo del host y comparte recursos con todos los contenedores del sistema.
- Comparte el kernel del host, pero aísla los procesos de la aplicación del resto del sistema.
- Requiere muchos menos recursos de hardware que las máquinas virtuales, por lo que los contenedores también se inician más rápido.
- Incluye todas las dependencias, como las dependencias del sistema y de programación, y los ajustes de configuración.



nota

Es posible que algunas aplicaciones no sean adecuadas para ejecutarse como un contenedor. Por ejemplo, en general, es posible que las aplicaciones que acceden a información de hardware de bajo nivel necesiten un acceso de hardware más directo que los contenedores.

Contenedores rootless y rootful

En el host de contenedores, puede ejecutar contenedores como usuario root o como usuario normal sin privilegios. Los contenedores que ejecuta un usuario con privilegios se denominan *contenedores rootful*. Los contenedores que ejecuta un usuario sin privilegios se denominan *contenedores rootless*.

Un contenedor rootless no puede usar recursos del sistema que generalmente están reservados para usuarios con privilegios, como el acceso a directorios restringidos o para publicar servicios de red en puertos restringidos (aquellos puertos por debajo de 1024). Esta función evita que un posible atacante obtenga privilegios de root en el host del contenedor.

Puede ejecutar contenedores directamente como `root`, si es necesario, pero este escenario debilita la seguridad del sistema si un error permite que un atacante comprometa el contenedor.

Diseño de arquitecturas basadas en contenedores

Los contenedores son una forma eficaz de volver a usar las aplicaciones alojadas y hacerlas portátiles. Los contenedores se pueden trasladar fácilmente de un entorno a otro, como de desarrollo a producción. Puede guardar varias versiones de un contenedor y acceder rápidamente a cada una según sea necesario.

Por lo general, los contenedores son temporales o efímeros. Puede guardar de forma permanente en un almacenamiento persistente los datos generados por un contenedor en ejecución, pero los contenedores, por lo general, se ejecutan cuando es necesario; luego, se detienen y se eliminan. Se inicia un nuevo proceso de contenedor la próxima vez que se necesita un contenedor en particular.

Podría instalar una aplicación de software compleja con varios servicios en un único contenedor. Por ejemplo, es posible que un servidor web necesite usar una base de datos y un sistema de mensajería. Sin embargo, el uso de un contenedor para varios servicios es difícil de administrar.

Un mejor diseño ejecuta en contenedores separados cada componente, el servidor web, la base de datos y el sistema de mensajería. De esta manera, las actualizaciones y el mantenimiento de los componentes de las aplicaciones individuales no afectan otros componentes ni la pila (stack) de aplicaciones.

Herramientas de administración de contenedores

Red Hat Enterprise Linux proporciona un conjunto de herramientas de contenedores que puede usar para ejecutar contenedores en un único servidor.

- `podman` administra contenedores e imágenes de contenedores.
- `skopeo` inspecciona, copia, elimina y firma imágenes.
- `buildah` crea imágenes de contenedores.

Estas herramientas son compatibles con Open Container Initiative (OCI). Con estas herramientas, usted puede administrar los contenedores de Linux creados por motores de contenedores compatibles con OCI, como Podman o Docker. Estas herramientas están diseñadas específicamente para ejecutar contenedores en Red Hat Enterprise Linux en un host de contenedores de un solo nodo.

En este capítulo, usará las utilidades `podman` y `skopeo` para ejecutar y administrar contenedores e imágenes de contenedores existentes.



nota

El uso de `buildah` para crear sus propias imágenes de contenedores no está incluido en el alcance de este curso, pero se trata en el curso de capacitación de Red Hat *Red Hat OpenShift I: Containers & Kubernetes* (DO180).

Imágenes de contenedores y registros

Para ejecutar contenedores, debe usar una *imagen de contenedor*. Una imagen de contenedor es un archivo estático que contiene pasos codificados y sirve como modelo para crear contenedores. Las imágenes de contenedor empaquetan una aplicación con todas sus dependencias, como las librerías del sistema, los tiempos de ejecución y las librerías del lenguaje de programación y otros valores de configuración.

Las imágenes de contenedores se compilan de acuerdo con las especificaciones, como la especificación de formato de imagen de Open Container Initiative (OCI). Estas especificaciones definen el formato para las imágenes de contenedores, así como los metadatos acerca de los sistemas operativos del host de contenedores y las arquitecturas de hardware que soporta la imagen.

Un *registro de contenedor* es un repositorio para almacenar y recuperar imágenes de contenedores. Un desarrollador envía o carga las imágenes de contenedores a un registro de contenedores. Puede extraer o descargar esas imágenes de contenedores del registro a un sistema local para ejecutar contenedores.

Puede usar un registro público que contenga imágenes de terceros o puede usar un registro privado controlado por su organización. El origen de las imágenes de contenedores es importante. Al igual que cualquier otro paquete de software, debe saber si puede confiar en el código de la imagen de contenedor. Las políticas varían entre registros sobre si proporcionan, evalúan y prueban las imágenes de contenedores que se les envían, y cómo lo hacen.

Red Hat distribuye las imágenes de contenedores certificadas a través de dos registros de contenedores principales a los que puede acceder con sus credenciales de inicio de sesión de Red Hat.

- `registry.redhat.io` para contenedores basados en productos oficiales de Red Hat.
- `registry.connect.redhat.com` para contenedores basados en productos de terceros.

Red Hat Container Catalog (<https://access.redhat.com/containers>) proporciona una interfaz web para buscar contenido certificado en estos registros.



nota

Red Hat proporciona la *imagen base universal (UBI)* como capa inicial para crear contenedores. La imagen de UBI es una imagen minimizada del contenedor que puede ser una primera capa para la compilación de una aplicación.

Necesita una cuenta de desarrollador de Red Hat para descargar una imagen de los registros de Red Hat. Puede usar el comando `podman login` para autenticarse en los registros. Si no proporciona una URL de registro al comando `podman login`, se autenticará en el registro configurado de forma predeterminada.

```
[user@host ~]$ podman login registry.lab.example.com
Username: RH134
Password: EXAMPLEPASSWORD
Login Succeeded!
```

También puede usar las opciones `--username` y `--password-stdin` del comando `podman login` para especificar el usuario y la contraseña para iniciar sesión en el registro. La opción `--password-stdin` lee la contraseña de `stdin`. Red Hat no recomienda usar la opción `--password`.

para proporcionar la contraseña directamente, ya que esta opción almacena la contraseña en los archivos de registro.

```
[user@host ~]# echo $PASSWORDVAR | podman login --username RH134 \
--password-stdin registry.access.redhat.com
```

Para verificar que haya iniciado sesión en un registro, use la opción `--get-login` del comando `podman login`.

```
[user01@rhel-vm ~]$ podman login registry.access.redhat.com --get-login
RH134
[user01@rhel-vm ~]$ podman login quay.io --get-login
Error: not logged into quay.io
```

En la salida anterior, la utilidad `podman` se autentica en el registro `registry.access.redhat.com` con las credenciales de usuario `RH134`, pero la utilidad `podman` no se autentica en el registro `quay.io`.

Configuración de registros de contenedores

El archivo de configuración predeterminado para los registros de contenedores es el archivo `/etc/containers/registries.conf`.

```
[user@host ~]$ cat /etc/containers/registries.conf
...output omitted...
[registries.search]
registries = ['registry.redhat.io', 'quay.io', 'docker.io']

# If you need to access insecure registries, add the registry's fully-qualified
# name.
# An insecure registry is one that does not have a valid SSL certificate or only
# does HTTP.
[registries.insecure]
registries = []
...output omitted...
```

Debido a que Red Hat recomienda usar un usuario sin privilegios para administrar contenedores, puede crear un archivo `registries.conf` para los registros de contenedores en el directorio `$HOME/.config/containers`. El archivo de configuración en este directorio anula la configuración en el archivo `/etc/containers/registries.conf`.

La lista de registros para buscar contenedores se configura en la sección `[registries.search]` de este archivo. Si especifica el nombre completo de una imagen de contenedor desde la línea de comandos, la utilidad de contenedor no busca en esta sección.

Los registros no seguros se enumeran en la sección `[registries.insecure]` del archivo `registries.conf`. Si un registro se detalla como no seguro, las conexiones a ese registro no están protegidas con cifrado TLS. Si un registro admite búsqueda y no es seguro, puede mostrarse en `[registries.search]` y en `[registries.insecure]`.

**nota**

En el aula se ejecuta un registro privado no seguro basado en Red Hat Quay para proporcionar imágenes de contenedores. Este registro satisface las necesidades del aula; sin embargo, no esperaría trabajar con registros inseguros en escenarios del mundo real. Para obtener más información sobre este software, consulte <https://access.redhat.com/products/red-hat-quay>.

Compilación de imágenes de contenedores con archivos de contenedores

Un *archivo contenedor* es un archivo de texto con instrucciones para compilar una imagen de contenedor. Un archivo contenedor generalmente tiene un *contexto* que define la ruta o URL donde se encuentran sus archivos y directorios. La imagen de contenedor resultante consta de capas de solo lectura, donde cada capa representa una instrucción del archivo contenedor.

La siguiente salida es un ejemplo de un archivo contenedor que usa la imagen de UBI del registro `registry.access.redhat.com`, instala el paquete `python3` e imprime la cadena `hello` en la consola.

```
[user@host ~]$ cat Containerfile
FROM registry.access.redhat.com/ubi8/ubi:latest
RUN dnf install -y python3
CMD ["/bin/bash", "-c", "echo hello"]
```

**nota**

La creación de un archivo contenedor y sus instrucciones de uso están fuera del alcance de este curso. Para obtener más información sobre los archivos de contenedor, consulte el curso DO180.

Administración de contenedores a escala

Las nuevas aplicaciones usan contenedores cada vez más para implementar componentes funcionales. Estos contenedores proporcionan servicios que consumen otras partes de la aplicación. En una organización, la administración de una cantidad cada vez mayor de contenedores puede convertirse rápidamente en una tarea abrumadora.

La implementación de contenedores a escala en la producción requiere un entorno que se puede adaptarse a los siguientes desafíos:

- La plataforma debe garantizar la disponibilidad de contenedores que proporcionen servicios esenciales.
- El entorno debe responder a los picos de uso de la aplicación mediante el aumento o la reducción de la cantidad de contenedores en ejecución y el balanceo de carga del tráfico.
- La plataforma debería detectar la falla de un contenedor o un host y reaccionar en consecuencia.
- Es posible que los desarrolladores necesiten un flujo de trabajo automatizado para ofrecer nuevas versiones de aplicaciones de forma transparente y segura.

Kubernetes es un servicio de orquestación que implementa, administra y escala aplicaciones basadas en contenedores en un clúster de hosts de contenedores. Kubernetes redirige el tráfico a sus contenedores con un balanceador de carga para que pueda escalar la cantidad de

contenedores que brindan un servicio. Kubernetes también soporta comprobaciones de estado definidas por el usuario para monitorear sus contenedores y reiniciarlos en caso de que fallen.

Red Hat proporciona una distribución de Kubernetes denominada *Red Hat OpenShift*. Red Hat OpenShift es un conjunto de componentes y servicios modulares desarrollado sobre la base de una infraestructura de Kubernetes. Ofrece características adicionales, como administración web remota, multiinquilino, monitoreo y auditoría, características avanzadas de seguridad, administración del ciclo de vida de la aplicación e instancias de autoservicio para desarrolladores.

Red Hat OpenShift no está incluido en el alcance de este curso, pero puede obtener más información sobre este en <https://www.openshift.com>.



nota

En una empresa, los contenedores individuales no se ejecutan generalmente desde la línea de comandos. En cambio, se prefiere ejecutar contenedores en producción mediante una plataforma basada en Kubernetes, como Red Hat OpenShift.

Sin embargo, es posible que necesite usar comandos para administrar contenedores e imágenes de forma manual o a escala pequeña. Este capítulo se centra en este caso de uso para comprender mejor los conceptos centrales (core) subyacentes de los contenedores, cómo funcionan y cómo pueden ser útiles.



Referencias

Páginas del manual `cgroups(7)`, `namespaces(7)`, `seccomp(2)`.

Especificación de imágenes de Open Container Initiative (OCI)

<https://github.com/opencontainers/image-spec/blob/master/spec.md>

Para obtener más información, consulte el capítulo *Starting with containers* de la *Red Hat Enterprise Linux 9 Building, Running, and Managing Containers Guide* en https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/building_running_and_managing_containers/index

► Cuestionario

Conceptos de contenedores

Elija las respuestas correctas para las siguientes preguntas:

- ▶ 1. **¿Qué herramienta de Red Hat Enterprise Linux ejecuta contenedores?**
 - a. buildah
 - b. container
 - c. podman
 - d. skopeo

- ▶ 2. **¿Cuáles dos enunciados describen la tecnología de contenedores? (Elija dos opciones).**
 - a. Los contenedores empaquetan sistemas operativos completos, con la adición de dependencias de librerías.
 - b. Los contenedores ejecutan procesos que están aislados del resto del sistema.
 - c. Cada contenedor incluye su propia versión del kernel y librerías.
 - d. Los contenedores proporcionan una forma estándar de empaquetar aplicaciones para facilitar la implementación y la administración.

- ▶ 3. **¿Cuáles dos enunciados son verdaderos sobre las imágenes de contenedores? (Elija dos opciones).**
 - a. Las imágenes de contenedores empaquetan una aplicación con todas las dependencias del tiempo de ejecución que necesita.
 - b. Las imágenes de contenedores que funcionan con Docker no pueden funcionar con Podman.
 - c. Las imágenes de contenedores solo se pueden ejecutar en un host de contenedores con la misma versión del software instalada en la imagen.
 - d. Las imágenes de contenedores sirven como modelos para crear contenedores.

- ▶ 4. **¿Cuáles son las tres tecnologías centrales (core) que se usan para implementar contenedores en Red Hat Enterprise Linux? (Elija tres opciones).**
 - a. Código de hipervisor para alojar máquinas virtuales.
 - b. Grupos de control (cgroups) para administrar recursos.
 - c. Espacios de nombres (Namespaces) para aislar procesos.
 - d. Sistema operativo completo para compatibilidad con el host de contenedores.
 - e. SELinux y Seccomp para la seguridad.

► 5. ¿Qué oración es verdadera acerca de los archivos contenedores?

- a. Un archivo contenedor es un archivo ejecutable que ejecuta un contenedor.
- b. Un archivo contenedor es un archivo ejecutable que compila una imagen de contenedor.
- c. Un archivo contenedor es un archivo comprimido que contiene librerías y configuración para un contenedor.
- d. Un archivo contenedor es un archivo de texto con instrucciones para compilar un contenedor.
- e. Un archivo contenedor es un archivo de texto con instrucciones para compilar una imagen de contenedor.

► Solución

Conceptos de contenedores

Elija las respuestas correctas para las siguientes preguntas:

- ▶ 1. **¿Qué herramienta de Red Hat Enterprise Linux ejecuta contenedores?**
 - a. buildah
 - b. container
 - c. podman
 - d. skopeo

- ▶ 2. **¿Cuáles dos enunciados describen la tecnología de contenedores? (Elija dos opciones).**
 - a. Los contenedores empaquetan sistemas operativos completos, con la adición de dependencias de librerías.
 - b. Los contenedores ejecutan procesos que están aislados del resto del sistema.
 - c. Cada contenedor incluye su propia versión del kernel y librerías.
 - d. Los contenedores proporcionan una forma estándar de empaquetar aplicaciones para facilitar la implementación y la administración.

- ▶ 3. **¿Cuáles dos enunciados son verdaderos sobre las imágenes de contenedores? (Elija dos opciones).**
 - a. Las imágenes de contenedores empaquetan una aplicación con todas las dependencias del tiempo de ejecución que necesita.
 - b. Las imágenes de contenedores que funcionan con Docker no pueden funcionar con Podman.
 - c. Las imágenes de contenedores solo se pueden ejecutar en un host de contenedores con la misma versión del software instalada en la imagen.
 - d. Las imágenes de contenedores sirven como modelos para crear contenedores.

- ▶ 4. **¿Cuáles son las tres tecnologías centrales (core) que se usan para implementar contenedores en Red Hat Enterprise Linux? (Elija tres opciones).**
 - a. Código de hipervisor para alojar máquinas virtuales.
 - b. Grupos de control (cgroups) para administrar recursos.
 - c. Espacios de nombres (Namespaces) para aislar procesos.
 - d. Sistema operativo completo para compatibilidad con el host de contenedores.
 - e. SELinux y Seccomp para la seguridad.

► 5. ¿Qué oración es verdadera acerca de los archivos contenedores?

- a. Un archivo contenedor es un archivo ejecutable que ejecuta un contenedor.
- b. Un archivo contenedor es un archivo ejecutable que compila una imagen de contenedor.
- c. Un archivo contenedor es un archivo comprimido que contiene librerías y configuración para un contenedor.
- d. Un archivo contenedor es un archivo de texto con instrucciones para compilar un contenedor.
- e. Un archivo contenedor es un archivo de texto con instrucciones para compilar una imagen de contenedor.

Implementación de contenedores

Objetivos

Analizar las herramientas de administración de contenedores para usar registros para almacenar y recuperar imágenes, y para implementar, consultar y acceder a contenedores.

La utilidad de Podman

Podman es un motor de contenedores con todas las funciones del metapquete `container-tools` para administrar contenedores e imágenes de *Open Container Initiative (OCI)*. La utilidad `podman` no usa un daemon para funcionar, por lo que los desarrolladores no necesitan una cuenta de usuario privilegiada en el sistema para iniciar o detener contenedores. Podman proporciona varios subcomandos para interactuar con contenedores e imágenes. En la siguiente lista, se muestran los subcomandos que se usan en esta sección:

Comandos de Podman

Comando	Descripción
<code>podman-build</code>	Compilar una imagen de contenedor con un archivo de contenedor.
<code>podman-run</code>	Ejecutar un comando en un nuevo contenedor.
<code>podman-images</code>	Enumerar las imágenes en el almacenamiento local.
<code>podman-ps</code>	Imprimir información sobre los contenedores.
<code>podman-inspect</code>	Mostrar la configuración de un contenedor, una imagen, un volumen, una red o un pod.
<code>podman-pull</code>	Descargar una imagen de un registro.
<code>podman-cp</code>	Copiar archivos o carpetas entre un contenedor y el sistema de archivos local.
<code>podman-exec</code>	Ejecutar un comando en un contenedor en ejecución.
<code>podman-rm</code>	Eliminar uno o más contenedores.
<code>podman-rmi</code>	Eliminar una o más imágenes almacenadas localmente.
<code>podman-search</code>	Buscar una imagen en un registro.

Para tratar los temas de esta clase, imagine el siguiente escenario.

Como administrador del sistema, debe ejecutar un contenedor que se basa en la imagen de contenedor de RHEL 8 UBI denominada `python38` con el paquete `python-38`. También tiene la tarea de crear una imagen de contenedor a partir de un archivo de contenedor y ejecutar un contenedor denominado `python36` desde esa imagen de contenedor. La imagen de contenedor que se crea con el archivo de contenedor debe tener la etiqueta `python36:1.0`. Identifique

las diferencias entre los dos contenedores. Además, asegúrese de que los paquetes `python` instalados en los contenedores no entren en conflicto con la versión de Python instalada en su máquina local.

Instalación de utilidades de contenedores

El metapaquete `container-tools` contiene las utilidades necesarias para interactuar con los contenedores y las imágenes de contenedores. Para descargar, ejecutar y comparar contenedores en su sistema, instale el metapaquete `container-tools` con el comando `dnf install`. Use el comando `dnf info` para visualizar la versión y el contenido del paquete `container-tools`.

```
[root@host ~]# dnf install container-tools
...output omitted...
[user@host ~]$ dnf info container-tools
...output omitted...
Summary      : A meta-package which container tools such as podman, buildah,
               : skopeo, etc.
License       : MIT
Description   : Latest versions of podman, buildah, skopeo, runc, common, CRIU,
               : Uidica, etc as well as dependencies such as container-selinux
               : built and tested together, and updated.
...output omitted...
```

El metapaquete `container-tools` proporciona las utilidades `podman` y `skopeo` necesarias para realizar las tareas asignadas.

Descarga de una imagen de contenedor desde un registro.

Primero, asegúrese de que la utilidad `podman` esté configurada para buscar y descargar contenedores del registro `registry.redhat.io`. El comando `podman info` muestra la información de configuración de la utilidad `podman`, incluidos sus registros configurados.

```
[user@host ~]$ podman info
...output omitted...
insecure registries:
  registries: []
registries:
  registries:
    - registry.redhat.io
    - quay.io
    - docker.io
...output omitted...
```

El comando `podman search` busca una imagen coincidente en la lista de registros configurados. De manera predeterminada, Podman busca en todos los registros de búsqueda no calificada. Según la API de distribución de Docker que se implemente con el registro, es posible que algunos registros no soporten la función de búsqueda.

Use el comando `podman search` para mostrar una lista de imágenes en los registros configurados que contienen el paquete `python-38`.

```
[user@host ~]$ podman search python-38
NAME                                     DESCRIPTION
registry.access.redhat.com/ubi7/python-38   Python 3.8 platform for building and
                                             running applications
registry.access.redhat.com/ubi8/python-38     Platform for building and running
                                             Python 3.8 applications
...output omitted...
```

La imagen `registry.access.redhat.com/ubi8/python-38` parece coincidir con los criterios para el contenedor requerido.

Puede usar el comando `skopeo inspect` para examinar diferentes formatos de imagen de contenedor desde un directorio local o un registro remoto sin descargar la imagen. La salida de este comando muestra una lista de las etiquetas de versión disponibles, los puertos expuestos de la aplicación contenerizada y los metadatos de la imagen de contenedor. Use el comando `skopeo inspect` para verificar que la imagen contenga el paquete `python-38` requerido.

```
[user@host ~]$ skopeo inspect docker://registry.access.redhat.com/ubi8/python-38
{
    "Name": "registry.access.redhat.com/ubi8/python-38",
    "Digest":
    "sha256:c6e522cba2cf2b3ae4a875d5210fb94aa1e7ba71b6cebd902a4f4df73cb090b8",
    "RepoTags": [
        ...output omitted...
        "1-68",
        "1-77-source",
        "latest"
    ...output omitted...
    "name": "ubi8/python-38",
    "release": "86.1648121386",
    "summary": "Platform for building and running Python 3.8 applications",
    ...output omitted...
    ...output omitted...
```

La imagen `registry.access.redhat.com/ubi8/python-38` contiene el paquete requerido y se basa en la imagen requerida. Use el comando `podman pull` para descargar la imagen seleccionada en la máquina local. Puede usar el nombre completo de la imagen de la salida anterior para evitar la ambigüedad en las versiones o registros del contenedor.

```
[user@host ~]$ podman pull registry.access.redhat.com/ubi8/python-38
Trying to pull registry.access.redhat.com/ubi8/python-38:latest...
Getting image source signatures
Checking if image destination supports signatures
Copying blob c530010fb61c done
...output omitted...
```

A continuación, use el comando `podman images` para mostrar las imágenes locales.

```
[user@host ~]$ podman images
REPOSITORY                                     TAG      IMAGE ID      CREATED       SIZE
registry.access.redhat.com/ubi8/python-38      latest   a33d92f90990  1 hour ago   901 MB
```

Creación de una imagen de contenedor a partir de un archivo de contenedor

Se le proporciona el siguiente archivo de contenedor para crear la imagen de contenedor en el directorio python36-app:

```
[user@host python36-app]$ cat Containerfile
FROM registry.access.redhat.com/ubi8/ubi:latest
RUN dnf install -y python36
CMD ["/bin/bash", "-c", "sleep infinity"]
```

El archivo contenedor anterior usa la imagen `registry.access.redhat.com/ubi8/ubi:latest` como imagen base. A continuación, el archivo contenedor instala el paquete `python36` y ejecuta el comando `sleep infinity` bash para evitar que el contenedor salga.

Normalmente, un contenedor ejecuta un proceso y, luego, sale después de que se completa ese proceso. El comando `sleep infinity` evita que el contenedor salga, ya que el proceso nunca se completa. A continuación, puede probar, desarrollar y depurar dentro del contenedor.

Después de examinar el archivo contenedor, use el comando `podman build` para compilar la imagen. El comando `podman build` crea una imagen de contenedor mediante el uso de instrucciones de uno o más archivos de contenedor. Debe estar en el directorio con el archivo contenedor para compilar la imagen con el comando `podman build`. Puede usar la opción `-t` del comando `podman build` para proporcionar el nombre y la etiqueta `python36:1.0` para la nueva imagen.

```
[user@host python36-app]$ podman build -t python36:1.0 .
STEP 1/3: FROM registry.access.redhat.com/ubi8/ubi:latest
STEP 2/3: RUN dnf install -y python36
...output omitted...
STEP 3/3: CMD ["/bin/bash", "-c", "sleep infinity"]
COMMIT python36:1.0
--> 35ab820880f
Successfully tagged localhost/python36:1.0
35ab820880f1708fa310f835407ffc94cb4b4fe2506b882c162a421827b156fc
```

La última línea de la salida anterior muestra el ID de la imagen del contenedor. La mayoría de los comandos de Podman usan los primeros 12 caracteres del ID de imagen de contenedor para hacer referencia a la imagen de contenedor. Puede usar este ID corto o el nombre de un contenedor o una imagen de contenedor como argumentos para la mayoría de los comandos de Podman.



nota

Si no se especifica un número de versión en la etiqueta, la imagen se crea con la etiqueta `:latest`. Si no se especifica un nombre de imagen, los campos de imagen y etiqueta muestran la cadena `<none>`.

Use el comando `podman images` para verificar que la imagen se crea con el nombre y la etiqueta definidos.

```
[user@host ~]$ podman images
REPOSITORY                                TAG      IMAGE ID      CREATED        SIZE
localhost/python36                           1.0      35ab820880f1  3 minute ago  266 MB
registry.access.redhat.com/ubi8/python-38    latest   a33d92f90990  1 hour ago   901 MB
```

A continuación, use el comando `podman inspect` para ver la información de bajo nivel de la imagen de contenedor y verificar que su contenido coincida con los requisitos del contenedor.

```
[user@host ~]$ podman inspect localhost/python36:1.0
...output omitted...
{
  "Cmd": [
    "/bin/bash",
    "-c",
    "sleep infinity"
  ],
  ...output omitted...
  {
    "created": "2022-04-18T19:47:52.708227513Z",
    "created_by": "/bin/sh -c dnf install -y python36",
    "comment": "FROM registry.access.redhat.com/ubi8/ubi:latest"
  },
  ...output omitted...
}
```

La salida del comando `podman inspect` muestra la imagen base `registry.access.redhat.com/ubi8/ubi:latest`, el comando `dnf` para instalar el paquete `python36` y el comando `bash sleep infinity` que se ejecuta en el tiempo de ejecución para evitar que el contenedor salga.



nota

La salida del comando `podman inspect` varía de la imagen `python-38` a la imagen `python36`, ya que creó la imagen `/python36` al agregar una capa con cambios a la imagen base `registry.access.redhat.com/ubi8/ubi:latest` existente, mientras que la imagen `python-38` es en sí misma una imagen base.

Ejecución de contenedores

Ahora que tiene las imágenes de contenedor requeridas, puede usarlas para ejecutar contenedores. Un contenedor puede estar en uno de los siguientes estados:

Creado

Un contenedor que se crea pero no se inicia.

En ejecución

Un contenedor que se está ejecutando con sus procesos.

Detenido

Un contenedor con sus procesos detenidos.

En pausa

Un contenedor con sus procesos en pausa. Sin soporte para contenedores rootless.

Eliminado

Un contenedor con sus procesos en estado inactivo.

capítulo 16 | Ejecución de contenedores

El comando `podman ps` enumera los contenedores en ejecución en el sistema. Use el comando `podman ps -a` para ver todos los contenedores (creados, detenidos, en pausa o en ejecución) en la máquina.

Use el comando `podman create` para crear el contenedor para ejecutarse más tarde. Para crear el contenedor, use el ID de la imagen de contenedor `localhost/python36`. También puede usar la opción `--name` para establecer un nombre para identificar el contenedor. La salida del comando es el ID largo del contenedor.

```
[user@host ~]$ podman create --name python36 dd6ca291f097  
c54c7ee281581c198cb96b07d78a0f94be083ae94dacbae69c05bd8cd354bbec
```

**nota**

Si no define un nombre para el contenedor con el comando `podman create` o `podman run` con la opción `--name`, la utilidad `podman` asigna un nombre aleatorio al contenedor.

A continuación, use los comandos `podman ps` y `podman ps -a` para verificar que el contenedor se haya creado pero no se haya iniciado. Puede ver información sobre el contenedor `python36`, como el ID corto, el nombre y el estado del contenedor, el comando que ejecuta cuando se inicia y la imagen para crear el contenedor.

```
[user@host ~]$ podman create --name python36 dd6ca291f097  
c54c7ee281581c198cb96b07d78a0f94be083ae94dacbae69c05bd8cd354bbec  
[user@host ~]$ podman ps  
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES  
[user@host ~]$ podman ps -a  
CONTAINER ID IMAGE COMMAND CREATED STATUS  
PORTS NAMES  
c54c7ee28158 localhost/python36:1.0 /bin/bash -c slee... 5 seconds ago Created  
python36
```

Ahora que verificó que el contenedor se creó correctamente, decide iniciar el contenedor, por lo que ejecuta el comando `podman start`. Puede usar el nombre o el ID del contenedor para iniciar el contenedor. La salida de este comando es el nombre del contenedor.

```
[user@host ~]$ podman start python36  
python36  
[user@host ~]$ podman ps  
CONTAINER ID IMAGE COMMAND CREATED STATUS  
PORTS NAMES  
c54c7ee28158 localhost/python36:1.0 /bin/bash -c slee... 6 minutes ago Up 3  
seconds ago python36
```

Ejecución de un contenedor desde un repositorio remoto

Puede usar el comando `podman run` para crear y ejecutar el contenedor más tarde. El comando `podman run` ejecuta un proceso dentro de un contenedor y este proceso inicia el nuevo contenedor.

Use la opción `-d` del comando `podman run` para ejecutar un contenedor en *modo separado*, que ejecuta el contenedor en segundo plano en lugar de primer plano de la sesión. En el ejemplo del contenedor `python36`, no necesita proporcionar un comando para que se ejecute el contenedor, ya que el comando `sleep infinity` ya se proporcionó en el archivo de contenedor que creó la imagen para ese contenedor.

Para crear el contenedor `python38`, usted opta por usar el comando `podman run` y hacer referencia a la imagen `registry.access.redhat.com/ubi8/python-38`. También opta por usar el comando `sleep infinity` para evitar que el contenedor salga.

```
[user@host ~]$ podman run -d --name python38 \
registry.access.redhat.com/ubi8/python-38 \
sleep infinity
a60f71a1dc1b997f5ef244aaed232e5de71dd1e8a2565428ccfebde73a2f9462
[user@host ~]$ podman ps
CONTAINER ID   IMAGE                               COMMAND
C54c7ee28158   localhost/python36:1.0             /bin/bash -c
slee... 37 minutes ago  Up 30 minutes ago          python36
a60f71a1dc1b   registry.access.redhat.com/ubi8/python-38:latest sleep infinity
32 seconds ago  Up 33 seconds ago                 python38
```



Importante

Si ejecuta un contenedor con el nombre completo de la imagen, pero la imagen aún no está almacenada localmente, el comando `podman run` primero extrae la imagen del registro y, luego, se ejecuta.

Aislamiento del entorno en contenedores

Los contenedores aíslan el entorno de una aplicación. Cada contenedor tiene su propio sistema de archivos, redes y procesos. Puede observar la función de aislamiento cuando observa la salida del comando `ps` y la compara entre la máquina host y un contenedor en ejecución.

Primero ejecuta el comando `ps -ax` en la máquina local y el comando devuelve un resultado esperado con muchos procesos.

```
[root@host ~]# ps -ax
 PID TTY      STAT   TIME COMMAND
  1 ?        Ss     0:01 /usr/lib/systemd/systemd --switched-root --system --
deseriali
  2 ?        S      0:00 [kthreadd]
  3 ?        I<    0:00 [rcu_gp]
  4 ?        I<    0:00 [rcu_par_gp]
...output omitted...
```

El comando `podman exec` ejecuta un comando en un contenedor en ejecución. El comando toma el nombre o ID del contenedor como primer argumento y los siguientes argumentos como comandos para ejecutarse dentro del contenedor. Use el comando `podman exec` para ver los procesos en ejecución en el contenedor `python36`. La salida del comando `ps aux` se ve diferente, ya que ejecuta procesos diferentes desde la máquina local.

```
[student@host ~]$ podman exec python38 ps -ax
  PID TTY      STAT   TIME COMMAND
    1 ?        Ss     0:00 /usr/bin/coreutils --coreutils-prog-shebang=sleep /
/usr/bin/sleep infinity
    7 ?        R      0:00 ps -ax
```

Puede usar el comando `sh -c` para encapsular el comando que se ejecutará en el contenedor. En el siguiente ejemplo, el comando `ps -ax > /tmp/process-data.log` se interpreta como el comando que se ejecutará en el contenedor. Si no encapsula el comando, Podman podría interpretar el carácter mayor que (`>`) como parte del comando `podman` en lugar de como un argumento para la opción `podman exec`.

```
[student@host ~]$ podman exec python38 sh -c 'ps -ax > /tmp/process-data.log'
  PID TTY      STAT   TIME COMMAND
    1 ?        Ss     0:00 /usr/bin/coreutils --coreutils-prog-shebang=sleep /
/usr/bin/sleep infinity
    7 ?        R      0:00 ps -ax
```

Usted decide comparar la versión instalada `python` en el sistema host con la versión instalada `python` en los contenedores.

```
[user@host ~]$ python3 --version
Python 3.9.10
[user@host ~]$ podman exec python36 python3 --version
Python 3.6.8
[user@host ~]$ podman exec python38 python3 --version
Python 3.8.8
```

Aislamiento de sistemas de archivos en contenedores

Los desarrolladores pueden usar la función de aislamiento del sistema de archivos para escribir y probar aplicaciones para diferentes versiones de lenguajes de programación sin la necesidad de usar varias máquinas físicas o virtuales.

Cree un script bash simple que muestre `Hello World` en el terminal en el directorio `/tmp`.

```
[user@host ~]$ echo "echo 'Hello World'" > /tmp/hello.sh
```

El archivo `/tmp/hello.sh` existe en la máquina host y no existe en el sistema de archivos dentro de los contenedores. Si intenta usar `podman exec` para ejecutar el script, se produce un error, ya que el script `/tmp/hello.sh` no existe en el contenedor.

```
[user@host ~]$ stat /tmp/hello.sh
  File: /tmp/hello.sh
  Size: 19          Blocks: 8          IO Block: 4096   regular file
Device: fc04h/64516d Inode: 17655599      Links: 1
Access: (0644/-rw-r--r--)  Uid: ( 1000/ user)  Gid: ( 1000/ user)
Context: unconfined_u:object_r:user_tmp_t:s0
Access: 2022-04-19 21:47:40.101601412 -0400
Modify: 2022-04-19 21:47:36.497558132 -0400
Change: 2022-04-19 21:47:36.497558132 -0400
 Birth: 2022-04-19 21:45:24.785976758 -0400
```

```
[user@host ~]$ podman exec python38 stat /tmp/hello.sh
stat: cannot statx '/tmp/hello.sh': No such file or directory
```

El comando `podman cp` copia archivos y carpetas entre los sistemas de archivos del host y del contenedor. Puede copiar el archivo `/tmp/hello.sh` en el contenedor `python38` con el comando `podman cp`.

```
[user@host ~]$ podman cp /tmp/hello.sh python38:/tmp/hello.sh

[user@host ~]$ podman exec python38 stat /tmp/hello.sh
  File: /tmp/hello.sh
  Size: 19          Blocks: 8          IO Block: 4096   regular file
Device: 3bh/59d Inode: 12280058      Links: 1
Access: (0644/-rw-r--r--)  Uid: ( 1001/ default)  Gid: (     0/    root)
Access: 2022-04-20 01:47:36.000000000 +0000
Modify: 2022-04-20 01:47:36.000000000 +0000
Change: 2022-04-20 02:02:04.732982187 +0000
 Birth: 2022-04-20 02:02:04.732982187 +0000
```

Una vez que se copia el script en el sistema de archivos del contenedor, se puede ejecutar desde el contenedor.

```
[user@host ~]$ podman exec python38 bash /tmp/hello.sh
hello world
```

Eliminación de contenedores e imágenes

Puede eliminar contenedores e imágenes con los comandos `podman rm` y `podman rmi`, respectivamente. Antes de eliminar una imagen de contenedor, se deben eliminar todos los contenedores en ejecución existentes de esa imagen.

Decide eliminar el contenedor `python38` y su imagen relacionada. Si intenta eliminar la imagen `registry.access.redhat.com/ubi8/python-38` mientras existe el contenedor `python38`, se produce un error.

```
[user@host ~]$ podman rmi registry.access.redhat.com/ubi8/python-38
Error: Image used by
a60f71a1dc1b997f5ef244aaed232e5de71dd1e8a2565428ccfebde73a2f9462: image is in use
by a container
```

Debe detener el contenedor para poder eliminarlo. Para detener un contenedor, use el comando `podman stop`.

```
[user@host ~]$ podman stop python38
```

Después de detener el contenedor, use el comando `podman rm` para eliminar el contenedor.

```
[user@host ~]$ podman rm python38
a60f71a1dc1b997f5ef244aaed232e5de71dd1e8a2565428ccfebde73a2f9462
```

Cuando el contenedor ya no existe, el `registry.access.redhat.com/ubi8/python-38` se puede eliminar con el comando `podman rmi`.

```
[user@host ~]$ podman rmi registry.access.redhat.com/ubi8/python-38
Untagged: registry.access.redhat.com/ubi8/python-38:latest
Deleted: a33d92f90990c9b1bad9aa98fe017e48f30c711b49527dcc797135352ea57d12
```



Referencias

Páginas del manual: `podman(1)`, `podman-build(1)`, `podman-cp(1)`, `podman-exec(1)`, `podman-images(1)`, `podman-inspect(1)`, `podman-ps(1)`, `podman-pull(1)`, `podman-rm(1)`, `podman-rmi(1)`, `podman-run(1)`, `podman-search(1)` y `podman-stop(1)`

Para obtener más información, consulte el capítulo Comenzar con contenedores en la Guía de creación, ejecución y administración de contenedores de Red Hat Enterprise Linux 9 en

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/building_running_and_managing_containers/index#starting-with-containers_building-running-and-managing-containers

► Ejercicio Guiado

Implementación de contenedores

En este ejercicio, usará herramientas de administración de contenedores para compilar una imagen, ejecutar un contenedor y consultar el entorno de contenedores en ejecución.

Resultados

- Configurar un registro de imágenes de contenedor y crear un contenedor a partir de una imagen existente.
- Creación de un contenedor a partir de un archivo de contenedor.
- Copiar un script de una máquina host en contenedores y ejecutar el script.
- Elimine los contenedores y las imágenes.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start containers-deploy
```

Instrucciones

- 1. Inicie sesión en la máquina `servera` como el usuario `student`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

- 2. Instale el metapaqete `container-tools`.

```
[student@servera ~]$ sudo dnf install container-tools
[sudo] password for student: student
...output omitted...
Is this ok [y/N]: y
...output omitted...
Complete!
```

- 3. Configure el registro del aula `registry.lab.example.com` en su directorio de inicio.
Inicie sesión en el registro de contenedor con el usuario `admin` y `redhat321` como contraseña.

- 3.1. Cree el directorio `/home/student/.config/containers`.

```
[student@servera ~]$ mkdir -p /home/student/.config/containers
```

- 3.2. Cree el archivo /home/student/.config/containers/registries.conf con el siguiente contenido:

```
unqualified-search-registries = ['registry.lab.example.com']

[[registry]]
location = "registry.lab.example.com"
insecure = true
blocked = false
```

- 3.3. Verifique que se haya agregado el registro del aula.

```
[student@servera ~]$ podman info
...output omitted...
registries:
  registry.lab.example.com:
    Blocked: false
    Insecure: true
    Location: registry.lab.example.com
    MirrorByDigestOnly: false
    Mirrors: null
    Prefix: registry.lab.example.com
search:
- registry.lab.example.com
...output omitted...
```

- 3.4. Inicie sesión en el registro del aula.

```
[student@servera ~]$ podman login registry.lab.example.com
Username: admin
Password: redhat321
Login Succeeded!
```

- 4. Ejecute el contenedor python38 en modo separado desde una imagen con el paquete python 3.8 y basado en la imagen ubi8. La imagen se aloja en un registro remoto.

- 4.1. Busque un contenedor python-38 en el registro registry.lab.example.com.

```
[student@servera ~]$ podman search registry.lab.example.com/
NAME                                     DESCRIPTION
...output omitted...
registry.lab.example.com/ubi8/python-38
registry.lab.example.com/ubi8/httpd-24
registry.lab.example.com/rhel8/php-74
```

- 4.2. Inspeccione la imagen.

```
[student@servera ~]$ skopeo inspect \
docker://registry.lab.example.com/ubi8/python-38
...output omitted...
  "description": "Python 3.8 available as container is a base platform for
building and running various Python 3.8 applications and frameworks.
...output omitted...
```

4.3. Extraiga la imagen de contenedor python-38.

```
[student@servera ~]$ podman pull registry.lab.example.com/ubi8/python-38
Trying to pull registry.lab.example.com/ubi8/python-38:latest...
...output omitted...
671cc3cb42984e338733ebb5a9a68e69e267cb7f9cb802283d3bc066f6321617
```

4.4. Verifique que el contenedor se descargue en el repositorio de imágenes local.

```
[student@servera ~]$ podman images
REPOSITORY                                     TAG      IMAGE ID      CREATED       SIZE
registry.lab.example.com/ubi8/python-38     latest   671cc3cb4298  5 days ago  901 MB
```

4.5. Inicie el contenedor python38.

```
[student@servera ~]$ podman run -d --name python38 \
registry.lab.example.com/ubi8/python-38 sleep infinity
004756b52d3d3326545f5075594cffa858afd474b903288723a3aa299e72b1af
```

4.6. Verifique que el contenedor se haya creado.

```
[student@servera ~]$ podman ps
CONTAINER ID  IMAGE                                     COMMAND
CREATED      STATUS          PORTS      NAMES
004756b52d3d  registry.lab.example.com/ubi8/python-38:latest  sleep infinity
About a minute ago  Up About a minute ago           python38
```

- 5. Compile una imagen de contenedor denominada python39:1.0 a partir de un archivo de contenedor y use la imagen para crear un contenedor denominado python39.

5.1. Examine el archivo del contenedor en el directorio /home/student/python39.

```
[student@servera ~]$ cat /home/student/python39/Containerfile
FROM registry.lab.example.com/ubi9-beta/ubi:latest
RUN echo -e '[rhel-9.0-for-x86_64-baseos-rpms]\nbaseurl = http://
content.example.com/rhel9.0/x86_64/dvd/BaseOS\nenabled = true\npgpcheck =
false\nname = Red Hat Enterprise Linux 9.0 BaseOS (dvd)\n[rhel-9.0-for-x86_64-
appstream-rpms]\nbaseurl = http://content.example.com/rhel9.0/x86_64/dvd/AppStream
\nenabled = true\npgpcheck = false\nname = Red Hat Enterprise Linux 9.0 Appstream
(dvd)'/>/etc/yum.repos.d/rhel_dvd.repo
RUN yum install --disablerepo=* --enablerepo=rhel-9.0-for-x86_64-baseos-rpms --
enablerepo=rhel-9.0-for-x86_64-appstream-rpms -y python3
```

capítulo 16 | Ejecución de contenedores

5.2. Cree una imagen de contenedor a partir de un archivo de contenedor.

```
[student@servera ~]$ podman build -t python39:1.0 /home/student/python39/.  
STEP 1/4: FROM registry.lab.example.com/ubi9-beta/ubi:latest  
...output omitted...  
STEP 2/4: RUN echo -e '[rhel-9.0-for-x86_64-baseos-rpms] ...  
...output omitted...  
STEP 3/4: RUN yum install --disablerepo=* --enablerepo=rhel-9.0-for-x86_64-baseos-  
rpms --enablerepo=rhel-9.0-for-x86_64-appstream-rpms -y python3  
...output omitted...  
STEP 4/4: CMD ["/bin/bash", "-c", "sleep infinity"]  
...output omitted...  
Successfully tagged localhost/python39:1.0  
80e68c195925beafe3b2ad7a54fe1e5673993db847276bc62d5f9d109e9eb499
```

5.3. Verifique que exista la imagen del contenedor en el repositorio de imágenes local.

```
[student@servera ~]$ podman images  
REPOSITORY                                TAG      IMAGE ID      CREATED        SIZE  
localhost/python39                          1.0      80e68c195925  3 minutes ago  266 MB  
registry.lab.example.com/ubi8/python-38     latest   671cc3cb4298  5 days ago    901 MB  
registry.lab.example.com/ubi9-beta/ubi       latest   fca12da1dc30  4 months ago   235 MB
```

5.4. Inspeccione el contenedor python39.

```
[student@servera ~]$ podman inspect localhost/python39:1.0  
...output omitted...  
  "comment": "FROM registry.lab.example.com/ubi9-beta/ubi:latest"  
...output omitted...  
  "created_by": "/bin/sh -c yum install --disablerepo=*  
--enablerepo=rhel-9.0-for-x86_64-baseos-rpms --enablerepo=rhel-9.0-for-x86_64-  
appstream-rpms -y python3"  
...output omitted...  
  "created_by": "/bin/sh -c #(nop) CMD [\"/bin/bash\", \"-c\", \"sleep  
infinity\"]",  
...output omitted...
```

5.5. Cree el contenedor python39.

```
[student@servera ~]$ podman create --name python39 localhost/python39:1.0  
3db4eabe9043224a7bdf195ab5fd810bf95db98dc29193392cef7b94489e1aae
```

5.6. Inicie el contenedor python39.

```
[student@servera ~]$ podman start python39  
python39
```

5.7. Verifique que el contenedor esté ejecutándose.

```
[student@servera ~]$ podman ps
CONTAINER ID  IMAGE                               COMMAND
CREATED      STATUS     PORTS      NAMES
004756b52d3d  registry.lab.example.com/ubi8/python-38:latest  sleep infinity
              33 minutes ago   Up 33 minutes ago
3db4eabe9043  localhost/python39:1.0           /bin/bash -c
              slee... About a minute ago   Up 42 seconds ago
                                         python39
```

- 6. Copie el script /home/student/script.py en el directorio /tmp de los contenedores en ejecución y ejecute el script en cada contenedor.

- 6.1. Copie el script de python /home/student/script.py en el directorio /tmp en ambos contenedores.

```
[student@servera ~]$ podman cp /home/student/script.py python39:/tmp/script.py
[student@servera ~]$ podman cp /home/student/script.py python38:/tmp/script.py
```

- 6.2. Ejecute el script de Python en ambos contenedores y, luego, ejecútelo en el host.

```
[student@servera ~]$ podman exec -it python39 python3 /tmp/script.py
This script was not run on the correct version of Python
Expected version of Python is 3.8
Current version of python is 3.9
[student@servera ~]$ podman exec -it python38 python3 /tmp/script.py
This script was correctly run on Python 3.8
[student@servera ~]$ python3 /home/student/script.py
This script was not run on the correct version of Python
Expected version of Python is 3.8
Current version of python is 3.9
```

- 7. Elimine los contenedores y las imágenes. Regrese a workstation.

- 7.1. Detenga ambos contenedores.

```
[student@servera ~]$ podman stop python39 python38
...output omitted...
python38
python39
```

- 7.2. Elimine ambos contenedores.

```
[student@servera ~]$ podman rm python39 python38
3db4eabe9043224a7bd195ab5fd810bf95db98dc29193392cef7b94489e1aae
004756b52d3d3326545f5075594cffa858afd474b903288723a3aa299e72b1af
```

- 7.3. Elimine ambas imágenes de contenedores.

```
[student@servera ~]$ podman rmi localhost/python39:1.0 \
registry.lab.example.com/ubi8/python-38:latest \
registry.lab.example.com/ubi9-beta/ubi
Untagged: localhost/python39:1.0
Untagged: registry.lab.example.com/ubi8/python-38:latest
Deleted: 80e68c195925beafe3b2ad7a54fe1e5673993db847276bc62d5f9d109e9eb499
Deleted: 219e43f6ff96fd11ea64f67cd6411c354dacbc5cbe296ff1fdbf5b717f01d89a
Deleted: 671cc3cb42984e338733ebb5a9a68e69e267cb7f9cb802283d3bc066f6321617
```

7.4. Regrese a workstation.

```
[student@servera ~]$ exit
logout
Connection to servera closed.
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish containers-deploy
```

Esto concluye la sección.

Administración del almacenamiento del contenedor y los recursos de red

Objetivos

Proporcionar almacenamiento persistente para los datos del contenedor al compartir el almacenamiento desde el host del contenedor y configurar una red de contenedores.

Administración de recursos del contenedor

Puede usar contenedores para ejecutar un proceso simple y salir. También puede configurar un contenedor para ejecutar un servicio de forma continua, como un servidor de base de datos. En este escenario, puede considerar agregar más recursos al contenedor, como el almacenamiento persistente o la resolución de DNS para otros contenedores.

Puede usar diferentes estrategias para configurar el almacenamiento persistente para contenedores. En una plataforma de contenedores empresarial, como Red Hat OpenShift, puede usar soluciones de almacenamiento sofisticadas para proporcionar almacenamiento a sus contenedores sin conocer la infraestructura subyacente.

Para implementaciones pequeñas en las que usa solo un host de contenedor, y sin la necesidad de escalar, puede crear almacenamiento persistente desde el host de contenedor mediante la creación de un directorio para montar en el contenedor en ejecución.

Cuando un contenedor, como un servidor web o un servidor de base de datos, proporciona contenido para clientes fuera del host del contenedor, debe configurar un canal de comunicación para que esos clientes accedan al contenido del contenedor. Puede configurar la *asignación de puertos* para habilitar la comunicación con un contenedor. Con la asignación de puertos, las solicitudes destinadas a un puerto en el host del contenedor se reenvían a un puerto dentro del contenedor.

Para tratar los temas de esta clase, imagine el siguiente escenario.

Como administrador del sistema, tiene la tarea de crear la base de datos contenerizada db01, basada en MariaDB, para usar la máquina local para permitir el tráfico del puerto 3306 con la configuración de firewall adecuada. El contenedor db01 debe usar almacenamiento persistente con el contexto de SELinux adecuado. Agregue la configuración de red adecuada para que el contenedor client01 pueda comunicarse con el contenedor db01 con DNS.

Variables del entorno para contenedores

Algunas imágenes de contenedor permiten el paso de variables de entorno para personalizar el contenedor en el momento de la creación. Puede usar variables de entorno para establecer parámetros en el contenedor para adaptarlo a su entorno sin la necesidad de crear su propia imagen personalizada. Por lo general, no modificaría la imagen del contenedor, ya que agregaría capas a la imagen, lo que podría ser más difícil de mantener.

Usa el comando `podman run -d registry.lab.example.com/rhel8/mariadb-105` para ejecutar una base de datos contenerizada, pero observa que el contenedor no se inicia.

```
[user@host ~]$ podman run -d registry.lab.example.com/rhel8/mariadb-105 \
--name db01
20751a03897f14764fb0e7c58c74564258595026124179de4456d26c49c435ad
[user@host ~]$ podman ps -a
CONTAINER ID IMAGE COMMAND
CREATED STATUS PORTS NAMES
20751a03897f registry.lab.example.com/rhel8/mariadb-105:latest run-mysqld
29 seconds ago Exited (1) 29 seconds ago db01
```

Usa el comando `podman container logs` para investigar el motivo del estado del contenedor.

```
[user@host ~]$ podman container logs db01
...output omitted...
You must either specify the following environment variables:
  MYSQL_USER (regex: '^[_a-zA-Z0-9]+$')
  MYSQL_PASSWORD (regex: '^[_a-zA-Z0-9_-!@#$%^&*()-=<>, .?;:|]+$')
  MYSQL_DATABASE (regex: '^[_a-zA-Z0-9]+$')
Or the following environment variable:
  MYSQL_ROOT_PASSWORD (regex: '^[_a-zA-Z0-9_-!@#$%^&*()-=<>, .?;:|]+$')
Or both.
...output omitted...
```

A partir de la salida anterior, determina que el contenedor no continuó ejecutándose porque las variables de entorno requeridas no se pasaron al contenedor. Por lo tanto, inspeccione la imagen de contenedor `mariadb-105` para encontrar más información acerca de las variables de entorno para personalizar el contenedor.

```
[user@host ~]$ skopeo inspect docker://registry.lab.example.com/rhel8/mariadb-105
...output omitted...
{
  "name": "rhel8/mariadb-105",
  "release": "40.1647451927",
  "summary": "MariaDB 10.5 SQL database server",
  "url": "https://access.redhat.com/containers/#/registry.access.redhat.com/rhel8/mariadb-105/images/1-40.1647451927",
  "usage": "podman run -d -e MYSQL_USER=user -e MYSQL_PASSWORD=pass -e MYSQL_DATABASE=db -p 3306:3306 rhel8/mariadb-105",
  "vcs-ref": "c04193b96a119e176ada62d779bd44a0e0edf7a6",
  "vcs-type": "git",
  "vendor": "Red Hat, Inc.",
  ...output omitted...
```

La etiqueta `usage` de la salida proporciona un ejemplo de cómo ejecutar la imagen. La etiqueta `url` apunta a una página web en Red Hat Container Catalog que documenta las variables de entorno y otra información acerca de cómo usar la imagen de contenedor.

La documentación para esta imagen muestra que el contenedor usa el puerto 3306 para el servicio de base de datos. La documentación también muestra que las siguientes variables de entorno están disponibles para configurar el servicio de base de datos:

Variables del entorno para la imagen mariadb

Variable	Descripción
MYSQL_USER	Nombre de usuario para la cuenta MySQL que se creará
MYSQL_PASSWORD	Contraseña para la cuenta de usuario
MYSQL_DATABASE	Nombre de la base de datos
MYSQL_ROOT_PASSWORD	Contraseña para el usuario root (opcional)

Después de examinar las variables de entorno disponibles para la imagen, use la opción `-e` del comando `podman run` para pasar variables de entorno al contenedor y use el comando `podman ps` para verificar que se esté ejecutando.

```
[user@host ~]$ podman run -d --name db01 \
-e MYSQL_USER=student \
-e MYSQL_PASSWORD=student \
-e MYSQL_DATABASE=dev_data \
-e MYSQL_ROOT_PASSWORD=redhat \
registry.lab.example.com/rhel8/mariadb-105
[user@host ~]$ podman ps
CONTAINER ID IMAGE COMMAND
CREATED STATUS PORTS NAMES
4b8f01be7fd6 registry.lab.example.com/rhel8/mariadb-105:latest run-mysqld 6
seconds ago Up 6 seconds ago db01
```

Almacenamiento persistente de contenedores

De manera predeterminada, el almacenamiento que usa un contenedor es efímero. La naturaleza efímera del almacenamiento en el contenedor significa que su contenido se pierde después de eliminar el contenedor. Debe tener en cuenta los permisos de nivel de sistema de archivos cuando monta un volumen persistente en un contenedor.

En la imagen MariaDB, el usuario `mysql` debe ser propietario del directorio `/var/lib/mysql`, al igual que si MariaDB se estuviera ejecutando en la máquina host. El directorio que desea montar en el contenedor debe tener `mysql` como el usuario y el propietario del grupo (o el UID/GID del usuario `mysql`, si MariaDB no está instalado en la máquina host). Si ejecuta un contenedor con el usuario `root`, los UID y GID en su máquina host coinciden con los UID y GID dentro del contenedor.

La configuración de coincidencia de UID y GID no se produce de la misma manera en un contenedor rootless. En un contenedor rootless, el usuario tiene acceso root desde dentro del contenedor, ya que Podman inicia un contenedor dentro del espacio de nombres del usuario.

Puede usar el comando `podman unshare` para ejecutar un comando dentro del espacio de nombres del usuario. Para obtener la asignación de UID para su espacio de nombres de usuario, use el comando `podman unshare cat`.

```
[user@host ~]$ podman unshare cat /proc/self/uid_map
 0      1000      1
 1      100000    65536
[user@host ~]$ podman unshare cat /proc/self/gid_map
 0      1000      1
 1      100000    65536
```

La salida anterior muestra que en el contenedor, el usuario root (UID y GID de 0) se asigna a su usuario (UID y GID de 1000) en la máquina host. En el contenedor, el UID y el GID de 1 se asignan al UID y al GID de 100000 en la máquina host. Cada UID y GID después de 1 se incrementa en 1. Por ejemplo, el UID y GID de 30 dentro de un contenedor se asigna al UID y GID de 100029 en la máquina host.

Use el comando `podman exec` para ver el UID y el GID del usuario `mysql` dentro del contenedor que se está ejecutando con almacenamiento efímero.

```
[user@host ~]$ podman exec -it db01 grep mysql /etc/passwd
mysql:x:27:27:MySQL Server:/var/lib/mysql:/sbin/nologin
```

Decide montar el directorio `/home/user/db_data` en el contenedor `db01` para proporcionar almacenamiento persistente en el directorio `/var/lib/mysql` del contenedor. A continuación, cree el directorio `/home/user/db_data` y use el comando `podman unshare` para establecer el UID y el GID del espacio de nombres de usuario de 27 como propietario del directorio.

```
[user@host ~]$ mkdir /home/user/db_data
[user@host ~]$ podman unshare chown 27:27 /home/user/db_data
```

El UID y el GID de 27 en el contenedor se asignan al UID y al GID de 100026 en la máquina host. Puede verificar la asignación al ver la propiedad del directorio `/home/user/db_data` con el comando `ls`.

```
[student@workstation ~]$ ls -l /home/user/
total 0
drwxrwxr-x. 3 100026 100026 18 May  5 14:37 db_data
...output omitted...
```

Ahora que se han establecido los permisos de nivel de sistema de archivos correctos, use la opción `-v` del comando `podman run` para montar el directorio.

```
[user@host ~]$ podman run -d --name db01 \
-e MYSQL_USER=student \
-e MYSQL_PASSWORD=student \
-e MYSQL_DATABASE=dev_data \
-e MYSQL_ROOT_PASSWORD=redhat \
-v /home/user/db_data:/var/lib/mysql \
registry.lab.example.com/rhel8/mariadb-105
```

Observa que el contenedor `db01` no se está ejecutando.

```
[user@host ~]$ podman ps -a
CONTAINER ID  IMAGE                                     COMMAND
CREATED      STATUS          PORTS     NAMES
dfdc20cf9a7e  registry.lab.example.com/rhel8/mariadb-105:latest  run-mysqld
29 seconds ago  Exited (1) 29 seconds ago               db01
```

El comando `podman container logs` muestra un error de permiso para el directorio `/var/lib/mysql/data`.

```
[user@host ~]$ podman container logs db01
...output omitted...
--> 16:41:25      Initializing database ...
--> 16:41:25      Running mysql_install_db ...
mkdir: cannot create directory '/var/lib/mysql/data': Permission denied
Fatal error Can't create database directory '/var/lib/mysql/data'
```

Este error ocurre debido al contexto de SELinux incorrecto que está configurado en el directorio `/home/user/db_data` en la máquina host.

Contextos de SELinux para almacenamiento en contenedores

Debe establecer el tipo de contexto de SELinux `container_file_t` para poder montar el directorio como almacenamiento persistente en un contenedor. Si el directorio no tiene el contexto `container_file_t` de SELinux, el contenedor no puede acceder al directorio. Puede agregar la opción `Z` al argumento de la opción `-v` del comando `podman run` para establecer automáticamente el contexto de SELinux en el directorio.

Por lo tanto, use el comando `podman run -v /home/user/dbfiles:/var/lib/mysql:Z` para establecer el contexto de SELinux para el directorio `/home/user/dbfiles` cuando lo monte como almacenamiento persistente para el directorio `/var/lib/mysql`.

```
[user@host ~]$ podman run -d --name db01 \
-e MYSQL_USER=student \
-e MYSQL_PASSWORD=student \
-e MYSQL_DATABASE=dev_data \
-e MYSQL_ROOT_PASSWORD=redhat \
-v /home/user/db_data:/var/lib/mysql:Z \
registry.lab.example.com/rhel8/mariadb-105
```

A continuación, verifica que el contexto SELinux correcto esté configurado en el directorio `/home/user/dbfiles` con la opción `-Z` del comando `ls`.

```
[user@host ~]$ ls -Z /home/user/
system_u:object_r:container_file_t:s0:c81,c1009 dbfiles
...output omitted...
```

Asignar una asignación de puertos a contenedores

Para proporcionar acceso de red a los contenedores, los clientes deben conectarse a los puertos en el host de contenedores que pasan el tráfico de red a través de los puertos en el contenedor. Cuando asigna un puerto de red en el host de contenedores a un puerto en el contenedor, el contenedor recibe el tráfico de red enviado al puerto de red del host.

capítulo 16 | Ejecución de contenedores

Por ejemplo, puede asignar el puerto 13306 en el host del contenedor al puerto 3306 en el contenedor para la comunicación con el contenedor MariaDB. Por lo tanto, el tráfico enviado al puerto del host de contenedores 13306 sería recibido por MariaDB que se ejecuta en el contenedor.

Use la opción `-p` del comando `podman run` para definir una asignación de puertos desde el puerto 13306 desde el host del contenedor al puerto 3306 en el contenedor `db01`.

```
[user@host ~]$ podman run -d --name db01 \
-e MYSQL_USER=student \
-e MYSQL_PASSWORD=student \
-e MYSQL_DATABASE=dev_data \
-e MYSQL_ROOT_PASSWORD=redhat \
-v /home/user/db_data:/var/lib/mysql:Z \
-p 13306:3306 \
registry.lab.example.com/rhel8/mariadb-105
```

Use la opción `-a` del comando `podman port` para mostrar todas las asignaciones de puertos de contenedores en uso. También puede usar el comando `podman port db01` para mostrar los puertos asignados para el contenedor `db01`.

```
[user@host ~]$ podman port -a
1c22fd905120 3306/tcp -> 0.0.0.0:13306
[user@host ~]$ podman port db01
3306/tcp -> 0.0.0.0:13306
```

Use el comando `firewall-cmd` para permitir el tráfico del puerto 13306 en la máquina host del contenedor para que pueda ser redirigido al contenedor.

```
[root@host ~]# firewall-cmd --add-port=13306/tcp --permanent
[root@host ~]# firewall-cmd --reload
```



Importante

Un contenedor rootless no puede abrir un puerto privilegiado (puertos inferiores a 1024) en el contenedor. Es decir, el comando `podman run -p 80:8080` normalmente no funciona para un contenedor rootless en ejecución. Para asignar un puerto en el host de contenedores inferior a 1024 a un puerto de contenedores, debe ejecutar Podman como usuario root o realizar otros ajustes en el sistema.

Puede asignar un puerto superior a 1024 en el host de contenedores a un puerto con privilegios en el contenedor, incluso si está ejecutando un contenedor rootless. La asignación de `8080:80` funciona si el contenedor proporciona un servicio que escucha en el puerto 80.

Configuración de DNS en un contenedor

Podman v4.0 soporta dos backends de red para contenedores: Netavark y CNI. A partir de RHEL 9, los sistemas usan Netavark de manera predeterminada. Para verificar qué backend de red se usa, ejecute el siguiente comando `podman info`.

```
[user@host ~]$ podman info --format {{.Host.NetworkBackend}}
netavark
```

**nota**

El metapquete `container-tools` incluye los paquetes `netavark` y `aardvark-dns`. Si Podman se instaló como un paquete independiente, o si el metapquete `container-tools` se instaló más tarde, el resultado del comando anterior podría ser `cni`. Para cambiar el backend de la red, defina la siguiente configuración en el archivo `/usr/share/containers/containers.conf`:

```
[network]
...output omitted...
network_backend = "netavark"
```

Los contenedores existentes en el host que usan la red Podman predeterminada no pueden resolver los nombres de host de los demás porque el DNS no está habilitado en la red predeterminada.

Use el comando `podman network create` para crear una red habilitada para DNS. Use el comando `podman network create` para crear la red denominada `db_net` y especifique la subred como `10.87.0.0/16` y la puerta de enlace como `10.87.0.1`.

```
[user@host ~]$ podman network create --gateway 10.87.0.1 \
--subnet 10.87.0.0/16 db_net
db_net
```

Si no especifica las opciones `--gateway` o `--subnet`, se crean con los valores predeterminados.

El comando `podman network inspect` muestra información acerca de una red específica. Use el comando `podman network inspect` para verificar que la puerta de enlace y la subred se hayan configurado correctamente y que la nueva red `db_net` esté habilitada para DNS.

```
[user@host ~]$ podman network inspect db_net
[
  {
    "name": "db_net",
    ...output omitted...
    "subnets": [
      {
        "subnet": "10.87.0.0/16",
        "gateway": "10.87.0.1"
      }
    ],
    ...output omitted...
    "dns_enabled": true,
    ...output omitted...
  ]
]
```

Puede agregar la red habilitada para DNS `db_net` a un nuevo contenedor con la opción `--network` del comando `podman run`. Use la opción `--network` del comando `podman run` para crear los contenedores `db01` y `client01` que están conectados a la red `db_net`.

```
[user@host ~]$ podman run -d --name db01 \
-e MYSQL_USER=student \
-e MYSQL_PASSWORD=student \
-e MYSQL_DATABASE=dev_data \
-e MYSQL_ROOT_PASSWORD=redhat \
-v /home/user/db_data:/var/lib/mysql:Z \
-p 13306:3306 \
--network db_net \
registry.lab.example.com/rhel8/mariadb-105
[user@host ~]$ podman run -d --name client01 \
--network db_net \
registry.lab.example.com/ubi8/ubi:latest \
sleep infinity
```

Debido a que los contenedores están diseñados para tener solo los paquetes mínimos requeridos, es posible que los contenedores no tengan las utilidades requeridas para probar la comunicación, como los comandos `ping` y `ip`. Puede instalar estas utilidades en el contenedor con el comando `podman exec`.

```
[user@host ~]$ podman exec -it db01 dnf install -y iputils iproute
...output omitted...
[user@host ~]$ podman exec -it client01 dnf install -y iputils iproute
...output omitted...
```

Los contenedores ahora pueden hacerse ping entre sí por nombre de contenedor. Pruebe la resolución de DNS con el comando `podman exec`. Los nombres se resuelven en las IP dentro de la subred que se configuró manualmente para la red `db_net`.

```
[user@host ~]$ podman exec -it db01 ping -c3 client01
PING client01.dns.podman (10.87.0.4) 56(84) bytes of data.
64 bytes from 10.87.0.4 (10.87.0.4): icmp_seq=1 ttl=64 time=0.049 ms
...output omitted...
--- client01.dns.podman ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 0.049/0.060/0.072/0.013 ms

[user@host ~]$ podman exec -it client01 ping -c3 db01
PING db01.dns.podman (10.87.0.3) 56(84) bytes of data.
64 bytes from 10.87.0.3 (10.87.0.3): icmp_seq=1 ttl=64 time=0.021 ms
...output omitted...
--- db01.dns.podman ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2047ms
rtt min/avg/max/mdev = 0.021/0.040/0.050/0.013 ms
```

Verifique que las direcciones IP en cada contenedor coincidan con la resolución de DNS con el comando `podman exec`.

```
[user@host ~]$ podman exec -it db01 ip a | grep 10.8
    inet 10.87.0.3/16 brd 10.87.255.255 scope global eth0
        inet 10.87.0.4/16 brd 10.87.255.255 scope global eth0
[user@host ~]$ podman exec -it client01 ip a | grep 10.8
    inet 10.87.0.3/16 brd 10.87.255.255 scope global eth0
        inet 10.87.0.4/16 brd 10.87.255.255 scope global eth0
```

Varias redes en un solo contenedor

Se pueden conectar varias redes a un contenedor al mismo tiempo para ayudar a separar diferentes tipos de tráfico.

Puede usar el comando `podman network create` para crear la red backend.

```
[user@host ~]$ podman network create backend
```

A continuación, use el comando `podman network ls` para ver todas las redes de Podman.

```
[user@host ~]$ podman network ls
NETWORK ID      NAME      DRIVER
a7fea510a6d1    backend    bridge
fe680efc5276    db01      bridge
2f259bab93aa    podman    bridge
```

La subred y la puerta de enlace no se especificaron con las opciones `--gateway` y `--subnet` del comando `podman network create`.

Use el comando `podman network inspect` para obtener la información IP de la red backend.

```
[user@host ~]$ podman network inspect backend
[
    {
        "name": "backend",
        ...output omitted...
        "subnets": [
            {
                "subnet": "10.89.1.0/24",
                "gateway": "10.89.1.1"
            }
        ]
    }
]
```

Puede usar el comando `podman network connect` para conectar redes adicionales a un contenedor cuando se está ejecutando. Puede usar el comando `podman network connect` para conectar la red backend a los contenedores `db01` y `client01`.

```
[user@host ~]$ podman network connect backend db01
[user@host ~]$ podman network connect backend client01
```

**Importante**

Si no se especifica una red con el comando `podman run`, el contenedor se conecta a la red predeterminada. La red predeterminada usa el modo de red `slirp4netns`, y las redes que crea con el comando `podman network create` usan el modo de red `puente`. Si intenta conectar una red de puente a un contenedor con el modo de red `slirp4netns`, el comando falla:

```
Error: "slirp4netns" is not supported: invalid network mode
```

Use el comando `podman inspect` para verificar que ambas redes estén conectadas a cada contenedor y para mostrar la información de IP.

```
[user@host ~]$ podman inspect db01
...output omitted...
    "backend": {
        "EndpointID": "",
        "Gateway": "10.89.1.1",
        "IPAddress": "10.89.1.4",
    },
    "db_net": {
        "EndpointID": "",
        "Gateway": "10.87.0.1",
        "IPAddress": "10.87.0.3",
    }
...output omitted...
[user@host ~]$ podman inspect client01
...output omitted...
    "backend": {
        "EndpointID": "",
        "Gateway": "10.89.1.1",
        "IPAddress": "10.89.1.5",
    },
    "db_net": {
        "EndpointID": "",
        "Gateway": "10.87.0.1",
        "IPAddress": "10.87.0.4",
    }
...output omitted...
```

El contenedor `client01` ahora puede comunicarse con el contenedor `db01` en ambas redes. Use el comando `podman exec` para hacer ping a ambas redes en el contenedor `db01` desde el contenedor `client01`.

```
[user@host ~]$ podman exec -it client01 ping -c3 10.89.1.4 | grep 'packet loss'
3 packets transmitted, 3 received, 0% packet loss, time 2052ms
[user@host ~]$ podman exec -it client01 ping -c3 10.87.0.3 | grep 'packet loss'
3 packets transmitted, 3 received, 0% packet loss, time 2054ms
```



Referencias

Páginas del manual: `podman(1)`, `podman-exec(1)`, `podman-info(1)`, `podman-network(1)`, `podman-network-create(1)`, `podman-network-inspect(1)`, `podman-network-ls(1)`, `podman-port(1)`, `podman-run(1)` y `podman-unshare(1)`

Para obtener más información, consulte el capítulo Trabajar con contenedores en la Guía de creación, ejecución y administración de contenedores de Red Hat Enterprise Linux 9 en

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/building_running_and_managing_containers/assembly_working-with-containers_building-running-and-managing-containers

► Ejercicio Guiado

Administración del almacenamiento del contenedor y los recursos de red

En este ejercicio, pasará variables de entorno a un contenedor durante la creación, montará almacenamiento persistente en un contenedor, creará y conectará varias redes de contenedores y expondrá puertos de contenedor desde la máquina host.

Resultados

- Crear redes de contenedores y conectarlas a contenedores.
- Solucionar problemas de contenedores fallidos.
- Pasar variables de entorno a contenedores durante la creación.
- Crear y montar almacenamiento persistente en contenedores.
- Asignar puertos de host a puertos dentro de contenedores.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start containers-resources
```

Instrucciones

- 1. Inicie sesión en la máquina `servera` como el usuario `student`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

- 2. Cree la red del contenedor `frontend`. Cree los contenedores `db_client` y `db_01` que está conectado a la red `frontend`.

- 2.1. Use las opciones `--subnet` y `--gateway` del comando `podman network create` para crear la red `frontend` con la subred `10.89.1.0/24` y la puerta de enlace `10.89.1.1`.

```
[student@servera ~]$ podman network create --subnet 10.89.1.0/24 \
--gateway 10.89.1.1 frontend
frontend
```

- 2.2. Inicie sesión en el registro `registry.lab.example.com`.

```
[student@servera ~]$ podman login registry.lab.example.com
Username: admin
Password: redhat321
Login Succeeded!
```

- 2.3. Cree el contenedor db_client que está conectado a la red frontend. Monte el directorio de repositorios DNF /etc/yum.repos.d dentro del contenedor en /etc/yum.repos.d para permitir la instalación de paquetes.

```
[student@servera ~]$ podman run -d --name db_client \
--network frontend \
-v /etc/yum.repos.d:/etc/yum.repos.d \
registry.lab.example.com/ubi9-beta/ubi \
sleep infinity
e20dfed7e392abe4b7bea3c25e9cb17ef95d16af9cedd50d68f997a663ba6c15
```

- 2.4. Cree el contenedor db_01 que está conectado a la red frontend.

```
[student@servera ~]$ podman run -d --name db_01 --network frontend \
registry.lab.example.com/rhel8/mariadb-105
3e767ae6eea4578152a216beb5ae98c8ef03a2d66098debe2736b8b458bab405
```

- 2.5. Ver todos los contenedores.

```
[student@servera ~]$ podman ps -a
CONTAINER ID  IMAGE                                     COMMAND
CREATED      STATUS          PORTS     NAMES
e20dfed7e392  registry.lab.example.com/ubi8/ubi:latest   sleep infinity
56 seconds ago Up 56 seconds ago           db_client
3e767ae6eea4  registry.lab.example.com/rhel8/mariadb-105:latest run-mysqld 1
second ago   Exited (1) 1 second ago           db_01
```

- 3. Solucione los problemas del contenedor db_01 y determine por qué no se está ejecutando. Vuelva a crear el contenedor db_01 con las variables de entorno requeridas.

- 3.1. Vea los registros del contenedor y determine por qué se cerró el contenedor.

```
[student@servera ~]$ podman container logs db_01
...output omitted...
You must either specify the following environment variables:
  MYSQL_USER (regex: '^[_a-zA-Z0-9_-]+$')
  MYSQL_PASSWORD (regex: '^[_a-zA-Z0-9_-~!@#$%^&*()-=;<,>,.;:|]+$')
  MYSQL_DATABASE (regex: '^[_a-zA-Z0-9_-]+$')
Or the following environment variable:
  MYSQL_ROOT_PASSWORD (regex: '^[_a-zA-Z0-9_-~!@#$%^&*()-=;<,>,.;:|]+$')
Or both.
...output omitted...
```

- 3.2. Elimine el contenedor db_01 y vuelva a crearlo con variables de entorno. Proporcione variables de entorno requeridas.

```
[student@servera ~]$ podman rm db_01  
3e767ae6eea4578152a216beb5ae98c8ef03a2d66098debe2736b8b458bab405  
[student@servera ~]$ podman run -d --name db_01 \  
--network frontend \  
-e MYSQL_USER=dev1 \  
-e MYSQL_PASSWORD=devpass \  
-e MYSQL_DATABASE=devdb \  
-e MYSQL_ROOT_PASSWORD=redhat \  
registry.lab.example.com/rhel8/mariadb-105  
948c4cd767b561432056e77adb261ab4024c1b66a22af17861aba0f16c66273b
```

3.3. Vea los contenedores en ejecución actuales.

```
[student@servera ~]$ podman ps  
CONTAINER ID IMAGE COMMAND  
CREATED STATUS PORTS NAMES  
e20dfed7e392 registry.lab.example.com/ubi8/ubi:latest sleep infinity  
56 seconds ago Up 56 seconds ago db_client  
948c4cd767b5 registry.lab.example.com/rhel8/mariadb-105:latest run-mysqld  
11 seconds ago Up 12 seconds ago db_01
```

- 4. Cree almacenamiento persistente para el servicio MariaDB contenerizada y asigne el puerto 13306 de la máquina local al puerto 3306 en el contenedor. Permita el tráfico al puerto 13306 en la máquina servera.

4.1. Cree el directorio /home/student/database en la máquina servera.

```
[student@servera ~]$ mkdir /home/student/databases
```

4.2. Obtenga el mysql UID y el GID del contenedor db_01 y, luego, elimine el contenedor db01.

```
[student@servera ~]$ podman exec -it db_01 grep mysql /etc/passwd  
mysql:x:27:27:MySQL Server:/var/lib/mysql:/sbin/nologin  
[student@servera ~]$ podman stop db_01  
db_01  
[student@servera ~]$ podman rm db_01  
948c4cd767b561432056e77adb261ab4024c1b66a22af17861aba0f16c66273b
```

4.3. Ejecute el comando chown dentro del espacio de nombres del contenedor y establezca el usuario y el propietario del grupo en 27 en el directorio /home/student/database.

```
[student@servera ~]$ podman unshare chown 27:27 /home/student/databases/  
[student@servera ~]$ ls -l /home/student/  
total 0  
drwxr-xr-x. 2 100026 100026 6 May 9 17:40 databases
```

4.4. Cree el contenedor db_01 y monte el directorio /home/student/databases desde la máquina servera al directorio /var/lib/mysql dentro del contenedor db_01. Use la opción Z para aplicar el contexto de SELinux requerido.

```
[student@servera ~]$ podman run -d --name db_01 \
--network frontend \
-e MYSQL_USER=dev1 \
-e MYSQL_PASSWORD=devpass \
-e MYSQL_DATABASE=devdb \
-e MYSQL_ROOT_PASSWORD=redhat \
-v /home/student/databases:/var/lib/mysql:Z \
-p 13306:3306 \
registry.lab.example.com/rhel8/mariadb-105
```

- 4.5. Instale el paquete mariadb en el contenedor db_client.

```
[student@servera ~]$ podman exec -it db_client dnf install -y mariadb
...output omitted...
Complete!
```

- 4.6. Cree la tabla crucial_data en la base de datos dev_db en el contenedor db_01 desde el contenedor db_client.

```
[student@servera ~]$ podman exec -it db_client mysql -u dev1 -p -h db_01
Enter password: devpass
...output omitted...
MariaDB [(none)]> USE devdb;
Database changed
MariaDB [devdb]> CREATE TABLE crucial_data(column1 int);
Query OK, 0 rows affected (0.036 sec)

MariaDB [devdb]> SHOW TABLES;
+-----+
| Tables_in_devdb |
+-----+
| crucial_data    |
+-----+
1 row in set (0.001 sec)

MariaDB [devdb]> quit
Bye
```

- 4.7. Permita el tráfico al puerto 13306 en el firewall en la máquina servera.

```
[student@servera ~]$ sudo firewall-cmd --add-port=13306/tcp --permanent
[sudo] password for student: student
success
[student@servera ~]$ sudo firewall-cmd --reload
success
```

- 4.8. Abra un segundo terminal en la máquina Workstation y use el cliente MariaDB para conectarse a la máquina servera en el puerto 13306 para mostrar las tablas en el contenedor db_01 que están almacenadas en el almacenamiento persistente.

```
[student@workstation ~]$ mysql -u dev1 -p -h servera --port 13306 \
devdb -e 'SHOW TABLES';
Enter password: devpass
+-----+
| Tables_in_devdb |
+-----+
| crucial_data     |
+-----+
```

- 5. Cree una segunda red de contenedores denominada backend y conecte la red backend a los contenedores db_client y db_01. Pruebe la conectividad de red y la resolución de DNS entre los contenedores.

- 5.1. Cree la red backend con la subred 10.90.0.0/24 y la puerta de enlace 10.90.0.1.

```
[student@servera ~]$ podman network create --subnet 10.90.0.0/24 \
--gateway 10.90.0.1 backend
backend
```

- 5.2. Conecte la red del contenedor backend a los contenedores db_client y db_01.

```
[student@servera ~]$ podman network connect backend db_client
[student@servera ~]$ podman network connect backend db_01
```

- 5.3. Obtenga las direcciones IP del contenedor db_01.

```
[student@servera ~]$ podman inspect db_01
...output omitted...
{
    "Networks": {
        "backend": {
            "EndpointID": "",
            "Gateway": "10.90.0.1",
            "IPAddress": "10.90.0.3",
        ...
        "frontend": {
            "EndpointID": "",
            "Gateway": "10.89.1.1",
            "IPAddress": "10.89.1.6",
        ...
    }
}
```

- 5.4. Instale el paquete iputils en el contenedor db_client.

```
[student@servera ~]$ podman exec -it db_client dnf install -y iputils
...output omitted...
Complete!
```

- 5.5. Haga ping al nombre del contenedor db_01 desde el contenedor db_client.

```
[student@servera ~]$ podman exec -it db_client ping -c4 db_01
PING db_01.dns.podman (10.90.0.3) 56(84) bytes of data.
...output omitted...
--- db_01.dns.podman ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3048ms
rtt min/avg/max/mdev = 0.043/0.049/0.054/0.004 ms
```

5.6. Salga de la máquina servera.

```
[student@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish containers-resources
```

Esto concluye la sección.

Administración de contenedores como servicios del sistema

Objetivos

Configurar un contenedor como servicio `systemd` y configurar un servicio de contenedor para que se inicie en el momento del arranque.

Administración de entornos de contenedores pequeños con unidades `systemd`

Puede ejecutar un contenedor para completar una tarea del sistema o para obtener la salida de una serie de comandos. También es posible que desee ejecutar contenedores que ejecutan un servicio de forma indefinida, como servidores web o bases de datos. En un entorno tradicional, un usuario con privilegios generalmente configura estos servicios para que se ejecuten en el arranque del sistema y los administra con el comando `systemctl`.

Como usuario regular, puede crear una unidad `systemd` para configurar sus contenedores rootless. Puede usar esta configuración para administrar su contenedor como un servicio del sistema regular con el comando `systemctl`.

La administración de contenedores basados en unidades `systemd` es principalmente útil para implementaciones básicas y pequeñas que no necesitan escalarse. Para un escalamiento y una orquestación más sofisticados de muchas aplicaciones y servicios basados en contenedores, puede usar una plataforma de orquestación empresarial basada en Kubernetes, como Red Hat OpenShift Container Platform.

Para analizar los temas de esta clase, imagine el siguiente escenario.

Como administrador del sistema, debe configurar el contenedor `webserver1` que se basa en la imagen de contenedor `http24` para iniciar un arranque del sistema. También debe montar el directorio `/app-artifacts` para el contenido del servidor web y asignar el puerto 8080 desde la máquina local al contenedor. Configure el contenedor para que se inicie y se detenga con los comandos `systemctl`.

Requisitos para los servicios de usuario de `systemd`

Como usuario regular, puede habilitar un servicio con el comando `systemctl`. El servicio se inicia cuando abre una sesión (interfaz gráfica, consola de texto o SSH) y se detiene cuando cierra la última sesión. Este comportamiento difiere de un servicio del sistema, que se inician cuando arranca el sistema y se detienen cuando el sistema se apaga.

De manera predeterminada, cuando crea una cuenta de usuario con el comando `useradd`, el sistema usa el siguiente ID disponible del rango de ID de usuario regular. El sistema también reserva un rango de ID para los contenedores del usuario en el archivo `/etc/subuid`. Si crea una cuenta de usuario con la opción `--system` del comando `useradd`, el sistema no reserva un rango para los contenedores de usuarios. Como consecuencia, no puede iniciar contenedores rootless con cuentas del sistema.

Decide crear una cuenta de usuario dedicada para administrar contenedores. Use el comando `useradd` para crear el usuario `appdev-adm` y use la contraseña `redhat`.

```
[user@host ~]$ sudo useradd appdev-adm
myapp.service
[user@host ~]$ sudo passwd appdev-adm
Changing password for user appdev-adm.
New password: redhat
BAD PASSWORD: The password is shorter than 8 characters
Retype new password: redhat
passwd: all authentication tokens updated successfully.
```

A continuación, use el comando `su` para cambiar al usuario `appdev-adm` y comience a usar el comando `podman`.

```
[user@host ~]$ su appdev-adm
Password: redhat
[appdev-adm@host ~]$ podman info
ERROR[0000] XDG_RUNTIME_DIR directory "/run/user/1000" is not owned by the current
user
[appdev-adm@host ~]$
```

Podman es una utilidad sin estado que requiere una sesión de inicio de sesión completa. Podman debe usarse dentro de una sesión SSH y no puede usarse en una shell `sudo` o `su`. Por lo tanto, salga de la shell `su` e inicie sesión en la máquina mediante SSH.

```
[appdev-adm@host ~]$ exit
[user@host ~]$ exit
[user@example ~]$ ssh appdev-adm@host
[appdev-adm@host ~]$
```

A continuación, configure el registro de contenedores y realice la autenticación con sus credenciales. Ejecute el contenedor `http` con el siguiente comando.

```
[appdev-adm@host ~]$ podman run -d --name webserver1 -p 8080:8080 -v \
~/app-artifacts:/var/www:Z registry.access.redhat.com/ubi8/httpd-24
af84e1ec33ea2f0d9787c56fbe7a62a4b9ce8ac03911be9e97f95575b306c297
[appdev-adm@host ~]$ podman ps -a
CONTAINER ID  IMAGE                                     COMMAND
CREATED      STATUS          PORTS          NAMES
af84e1ec33ea  registry.access.redhat.com/ubi8/httpd-24:latest /usr/bin/run-
http...  16 seconds ago  Exited (1) 15 seconds ago  0.0.0.0:8080->8080/tcp
webserver1
```

Observa que el contenedor `webserver1` no se inició, por lo que ejecuta el comando `podman container logs` para ver los registros del contenedor.

```
[appdev-adm@host ~]$ podman container logs webserver1
=> sourcing 10-set-mpm.sh ...
=> sourcing 20-copy-config.sh ...
=> sourcing 40-ssl-certs.sh ...
---> Generating SSL key pair for httpd...
AH00526: Syntax error on line 122 of /etc/httpd/conf/httpd.conf:
DocumentRoot '/var/www/html' is not a directory, or is not readable
[appdev-adm@servera ~]$
```

Los registros del contenedor `webserver1` muestran que el archivo `/var/www/html` no se puede leer. Este error se produce porque el directorio de montaje del contenedor no puede encontrar el subdirectorio `html`. Puede eliminar el contenedor existente, actualizar el comando y ejecutarlo de la siguiente manera:

```
[appdev-adm@host ~]$ podman run -d --name webserver1 -p 8080:8080 -v \
~/app-artifacts:/var/www/html:Z registry.access.redhat.com/ubi8/httpd-24
cde4a3d8c9563fd50cc39de8a4873dcf15a7e881ba4548d5646760eae7a35d81
[appdev-adm@host ~]$ podman ps
CONTAINER ID  IMAGE                                     COMMAND
CREATED      STATUS          PORTS          NAMES
cde4a3d8c956  registry.access.redhat.com/ubi8/httpd-24:latest  /usr/bin/run-
http...  4 seconds ago  Up 5 seconds ago  0.0.0.0:8080->8080/tcp  webserver1
```

Creación de archivos usuarios `systemd` para contenedores.

Puede definir manualmente `systemd` servicios en el directorio `~/.config/systemd/user/`. La sintaxis de archivos para los servicios de usuario es la misma que para los archivos de servicios del sistema. Para obtener más detalles, consulte las páginas del manual `systemd.unit(5)` y `systemd.service(5)`.

Use el comando `podman generate systemd` para generar archivos de servicio `systemd` para un contenedor existente. El comando `podman generate systemd` usa un contenedor como modelo para crear el archivo de configuración.

La opción `--new` del comando `podman generate systemd` le indica a la utilidad `podman` que configure el servicio `systemd` para crear el contenedor cuando se inicie el servicio y eliminarlo cuando este se detenga.



Importante

Sin la opción `--new`, la utilidad `podman` configura el archivo de unidad del servicio para iniciar y detener el contenedor existente sin eliminarlo.

Use el comando `podman generate systemd` con la opción `--name` para mostrar el archivo de servicio `systemd` que se modela para el contenedor `webserver1`.

```
[appdev-adm@host ~]$ podman generate systemd --name webserver1
...output omitted...
ExecStart=/usr/bin/podman start webserver1 ①
ExecStop=/usr/bin/podman stop -t 10 webserver1 ②
ExecStopPost=/usr/bin/podman stop -t 10 webserver1
...output omitted...
```

- ① En start (iniciar), el daemon `systemd` ejecuta el comando `podman start` para iniciar el contenedor existente.
- ② En stop (detener), el daemon `systemd` ejecuta el comando `podman stop` para detener el contenedor. Tenga en cuenta que el daemon `systemd` no elimina el contenedor en esta acción.

A continuación, use el comando anterior con la opción `--new` para comparar la configuración `systemd`.

```
[appdev-adm@host ~]$ podman generate systemd --name webserver1 --new
...output omitted...
ExecStartPre=/bin/rm -f %t/%n.ctr-id
ExecStart=/usr/bin/podman run --cidfile=%t/%n.ctr-id --cgroups=no-common --rm --
sdnotify=common --replace -d --name webserver1 -p 8080:8080 -v /home/appdev-adm/
app-artifacts:/var/www/html:Z registry.access.redhat.com/ubi8/httpd-24 ①
ExecStop=/usr/bin/podman stop --ignore --cidfile=%t/%n.ctr-id ②
ExecStopPost=/usr/bin/podman rm -f --ignore --cidfile=%t/%n.ctr-id ③
...output omitted...
```

- ① En start (iniciar), el daemon `systemd` ejecuta el comando `podman run` para crear y, luego, iniciar un nuevo contenedor. Esta acción usa la opción `--rm` del comando `podman run` que elimina el contenedor al detenerse.
- ② En stop (detener), `systemd` ejecuta el comando `podman stop` para detener el contenedor.
- ③ Después de que `systemd` haya detenido el contenedor, `systemd` lo elimina mediante el comando `podman rm -f`.

Verifique la salida del comando `podman generate systemd` y ejecute el comando anterior con la opción `--files` para crear el archivo de usuario `systemd` en el directorio actual. Debido a que el contenedor `webserver1` usa el almacenamiento persistente, usted opta por usar el comando `podman generate systemd` con la opción `--new`. A continuación, cree el directorio `~/.config/systemd/user/` y mueva el archivo a esta ubicación.

```
[appdev-adm@host ~]$ podman generate systemd --name webserver1 --new --files
/home/appdev-adm/container-webserver1.service
[appdev-adm@host ~]$ mkdir -p ~/.config/systemd/user/
[appdev-adm@host ~]$ mv container-webserver1.service ~/.config/systemd/user/
```

Administración de archivos usuarios `systemd` para contenedores.

Ahora que creó el archivo de usuario `systemd`, puede usar la opción `--user` del comando `systemctl` para administrar el contenedor `webserver1`.

capítulo 16 | Ejecución de contenedores

Primero, recargue el daemon `systemd` para que el comando `systemctl` conozca el nuevo archivo de usuario. Use el comando `systemctl --user start` para iniciar el contenedor `webserver1`. Use el nombre del archivo de usuario `systemd` generado para el contenedor.

```
[appdev-adm@host ~]$ systemctl --user start container-webserver1.service
[appdev-adm@host ~]$ systemctl --user status container-webserver1.service
● container-webserver1.service - Podman container-webserver1.service
   Loaded: loaded (/home/appdev-adm/.config/systemd/user/container-
webserver1.service; disabled; vendor preset: disabled)
     Active: active (running) since Thu 2022-04-28 21:22:26 EDT; 18s ago
       Docs: man:podman-generate-systemd(1)
    Process: 31560 ExecStartPre=/bin/rm -f /run/user/1003/container-
webserver1.service.ctr-id (code=exited, status=0/SUCCESS)
      Main PID: 31600 (common)
     ...output omitted...
[appdev-adm@host ~]$ podman ps
CONTAINER ID  IMAGE                                     COMMAND
CREATED      STATUS          PORTS          NAMES
18eb00f42324  registry.access.redhat.com/ubi8/httpd-24:latest  /usr/bin/run-
http... 28 seconds ago  Up 29 seconds ago  0.0.0.0:8080->8080/tcp  webserver1
Created symlink /home/appdev-adm/.config/systemd/user/default.target.wants/
container-webserver1.service → /home/appdev-adm/.config/systemd/user/container-
webserver1.service.
```

**Importante**

Al configurar un contenedor con el daemon `systemd`, el daemon monitorea el estado del contenedor y lo reinicia si falla. No use el comando `podman` para iniciar o detener estos contenedores. Si lo hace, puede interferir con el monitoreo del daemon `systemd`.

En la siguiente tabla, se resumen los diferentes directorios y comandos que se usan entre los servicios de usuario y del sistema `systemd`.

Comparación de servicios de usuario y del sistema

Almacenamiento de archivos de unidad personalizados	Servicios del sistema	<code>/etc/systemd/system/unit.service</code>
	Servicios de usuario	<code>~/.config/systemd/user/unit.service</code>
Recarga de archivos de unidad	Servicios del sistema	<code># systemctl daemon-reload</code>
	Servicios de usuario	<code>\$ systemctl --user daemon-reload</code>
Inicio y detención de un servicio	Servicios del sistema	<code># systemctl start UNIT</code> <code># systemctl stop UNIT</code>

	Servicios de usuario	<code>\$ systemctl --user start UNIT</code> <code>\$ systemctl --user stop UNIT</code>
Inicio de un servicio cuando se inicia la máquina	Servicios del sistema	<code># systemctl enable UNIT</code>
	Servicios de usuario	<code>\$ loginctl enable-linger</code> <code>\$ systemctl --user enable UNIT</code>

Configuración de contenedores para que se inicien en el arranque del sistema

Ahora que la configuración `systemd` para el contenedor está completa, sale de la sesión SSH. Algun tiempo después, se le notifica que el contenedor se detiene después de salir de la sesión.

Puede cambiar este comportamiento predeterminado y obligar a los servicios habilitados a que se inicien con el servidor y se detengan durante el apagado mediante la ejecución del comando `loginctl enable-linger`.

Use el comando `loginctl` para configurar el servicio de usuario `systemd` para que persista después de que se cierre la última sesión de usuario del servicio configurado. A continuación, verifique la configuración correcta con el comando `loginctl show-user`.

```
[user@host ~]$ loginctl show-user appdev-adm
...output omitted...
Linger=no
[user@host ~]$ loginctl enable-linger
[user@host ~]$ loginctl show-user appdev-adm
...output omitted...
Linger=yes
```

Para revertir la operación, use el comando `loginctl disable-linger`.

Administración de contenedores como root con `systemd`

También puede configurar contenedores para que se ejecuten como root y administrarlos con los archivos de servicio `systemd`. Una de las ventajas de este enfoque es que puede configurar los archivos de unidad para que funcionen exactamente igual que los archivos de unidad `systemd` normales, en lugar de como un usuario en particular.

El procedimiento para definir el archivo de servicio como root es similar al procedimiento descrito anteriormente para contenedores rootless, con las siguientes excepciones:

- No cree un usuario dedicado para la administración de contenedores.
- El archivo de servicio debe estar en el directorio `/etc/systemd/system` en lugar del directorio `~/.config/systemd/user`.
- Los contenedores se administran con el comando `systemctl` sin la opción `--user`.
- No ejecute el comando `loginctl enable-linger` con el usuario `root`.

Para obtener una demostración, consulte el video de YouTube del canal de videos de Red Hat que se detalla en las referencias al final de esta sección.



Referencias

Páginas del manual `logindctl(1)`, `systemd.unit(5)`, `systemd.service(5)`, `subuid(5)` y `podman-generate-systemd(1)`

Administración de contenedores en Podman con archivos de unidad systemd

<https://www.youtube.com/watch?v=AGkM2jGT61Y>

Para obtener más información, consulte el capítulo *Running Containers as Systemd Services with Podman* de la *Red Hat Enterprise Linux 9 Building, Running, and Managing Containers Guide* en

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/building_running_and_managing_containers/index

► Ejercicio Guiado

Administración de contenedores como servicios del sistema

En este ejercicio, configurará un contenedor para administrar como un servicio `systemd` y, luego, usa los comandos `systemctl` para administrar ese contenedor, de modo que se inicie automáticamente cuando se inicia la máquina host.

Resultados

- Crear archivos de servicio `systemd` para administrar un contenedor.
- Configurar un contenedor para que pueda administrarlo con los comandos `systemctl`.
- Configurar cuentas de usuario para que los servicios de usuario `systemd` inicien un contenedor cuando se inicia la máquina host.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start containers-services
```

Instrucciones

- 1. Inicie sesión en la máquina `servera` como el usuario `student`.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

- 2. Cree una cuenta de usuario denominada `contsvc` y use `redhat` como contraseña. Use esta cuenta de usuario para ejecutar contenedores como servicios `systemd`.

- 2.1. Cree el usuario `contsvc`. Establezca `redhat` como contraseña para el usuario `contsvc`.

```
[student@servera ~]$ sudo useradd contsvc
[sudo] password for student: student
[student@servera ~]$ sudo passwd contsvc
Changing password for user contsvc.
New password: redhat
BAD PASSWORD: The password is shorter than 8 characters
Retype new password: redhat
passwd: all authentication tokens updated successfully.
```

- 2.2. Para administrar los servicios de usuario `systemd` con la cuenta `contsvc`, debe iniciar sesión directamente con el usuario `contsvc`. No puede usar los comandos `su` y `sudo` para crear una sesión con el usuario `contsvc`.

Regrese a la máquina `workstation` como el usuario `student` y, luego, inicie sesión como el usuario `contsvc`.

```
[student@servera ~]$ exit  
logout  
Connection to servera closed.  
[student@workstation ~]$ ssh contsvc@servera  
...output omitted...  
[contsvc@servera ~]$
```

- 3. Configure el acceso al registro del aula `registry.lab.example.com` en su directorio de inicio. Use el archivo `/tmp/containers-services/registries.conf` como plantilla.

- 3.1. Cree el directorio `~/.config/containers/`.

```
[contsvc@servera ~]$ mkdir -p ~/.config/containers/
```

- 3.2. El script `lab` prepara el archivo `registries.conf` en el directorio `/tmp/containers-services/`. Copie ese archivo en el directorio `~/.config/containers/`.

```
[contsvc@servera ~]$ cp /tmp/containers-services/registries.conf \  
~/.config/containers/
```

- 3.3. Verifique que pueda acceder al registro `registry.lab.example.com`. Si todo funciona según lo previsto, el comando debe enumerar algunas imágenes.

```
[contsvc@servera ~]$ podman search ubi  
NAME                                     DESCRIPTION  
registry.lab.example.com/ubi7/ubi  
registry.lab.example.com/ubi8/ubi  
registry.lab.example.com/ubi9-beta/ubi
```

- 4. Use el directorio `/home/contsvc/webcontent/html/` como almacenamiento persistente para el contenedor del servidor web. Cree la página de prueba `index.html` con la línea `Hello World` dentro del directorio.

- 4.1. Cree el directorio `~/webcontent/html/`.

```
[contsvc@servera ~]$ mkdir -p ~/webcontent/html/
```

- 4.2. Cree el archivo `index.html` y agregue la línea `Hello World`.

```
[contsvc@servera ~]$ echo "Hello World" > ~/webcontent/html/index.html
```

- 4.3. Confirme que el permiso para otros esté definido en `r--` en el archivo `index.html`. El contenedor usa un usuario sin privilegios que debe ser capaz de leer el archivo `index.html`.

```
[contsvc@servera ~]$ ls -ld webcontent/html/
drwxr-xr-x. 2 contsvc contsvc 24 Aug 28 04:56 webcontent/html/
[contsvc@servera ~]$ ls -l webcontent/html/index.html
-rw-r--r--. 1 contsvc contsvc 12 Aug 28 04:56 webcontent/html/index.html
```

- 5. Use la imagen `registry.lab.example.com/rhel8/httpd-24:1-105` para ejecutar un contenedor denominado `webapp` en modo separado. Redirija el puerto 8080 en el host local al puerto del contenedor 8080. Monte el directorio `~/webcontent` desde el host en el directorio `/var/www` del contenedor.
- 5.1. Inicie sesión en el registro `registry.lab.example.com` con el usuario `admin` y `redhat321` como contraseña.

```
[contsvc@servera ~]$ podman login registry.lab.example.com
Username: admin
Password: redhat321
Login Succeeded!
```

- 5.2. Use la imagen `registry.lab.example.com/rhel8/httpd-24:1-163` para ejecutar un contenedor denominado `webapp` en modo separado. Use la opción `-p` para asignar el puerto 8080 en `servera` al puerto 8080 en el contenedor. Use la opción `-v` para montar el directorio `~/webcontent` en `servera` para el directorio `/var/www` en el contenedor.

```
[contsvc@servera ~]$ podman run -d --name webapp -p 8080:8080 -v \
~/webcontent:/var/www:Z registry.lab.example.com/rhel8/httpd-24:1-163
750a681bd37cb6825907e9be4347eec2c4cd79550439110fc6d41092194d0e06
...output omitted...
```

- 5.3. Verifique que el servicio web esté funcionando en el puerto 8080.

```
[contsvc@servera ~]$ curl http://localhost:8080
Hello World
```

- 6. Cree un archivo de servicio `systemd` para administrar el contenedor `webapp` con los comandos `systemctl`. Configure el servicio `systemd` para que cuando inicie el servicio, el daemon `systemd` cree un contenedor. Después de finalizar la configuración, detenga y elimine el contenedor `webapp`. Recuerde que el daemon `systemd` espera que el contenedor no exista inicialmente.

- 6.1. Cree y cambie el directorio `~/.config/systemd/user/`.

```
[contsvc@servera ~]$ mkdir -p ~/.config/systemd/user/
[contsvc@servera ~]$ cd ~/.config/systemd/user
```

- 6.2. Cree el archivo de unidad para el contenedor `webapp`. Use la opción `--new` para que `systemd` cree un contenedor al iniciar el servicio y elimine el contenedor al detenerlo.

```
[contsvc@servera user]$ podman generate systemd --name webapp --files --new
/home/contsvc/.config/systemd/user/container-webapp.service
```

6.3. Detenga y, luego, elimine el contenedor webapp.

```
[contsvc@servera user]$ podman stop webapp
webapp
[contsvc@servera user]$ podman rm webapp
750a681bd37cb6825907e9be4347eec2c4cd79550439110fc6d41092194d0e06
[contsvc@servera user]$ podman ps -a
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
```

- 7. Vuelva a cargar la configuración del daemon `systemd` y, luego, habilite e inicie su nuevo servicio de usuario `container-webapp`. Verifique la configuración del servicio `systemd`, detenga e inicie el servicio y muestre la respuesta del servidor web y el estado del contenedor.

7.1. Recargue la configuración para reconocer el nuevo archivo de unidad.

```
[contsvc@servera user]$ systemctl --user daemon-reload
```

7.2. Habilite e inicie el servicio `container-webapp`.

```
[contsvc@servera user]$ systemctl --user enable --now container-webapp
Created symlink /home/contsvc/.config/systemd/user/multi-user.target.wants/
container-webapp.service → /home/contsvc/.config/systemd/user/container-
webapp.service.
Created symlink /home/contsvc/.config/systemd/user/default.target.wants/container-
webapp.service → /home/contsvc/.config/systemd/user/container-webapp.service.
```

7.3. Verifique que el servidor web responda a solicitudes.

```
[contsvc@servera user]$ curl http://localhost:8080
Hello World
```

7.4. Verifique que el contenedor esté ejecutándose.

```
[contsvc@servera user]$ podman ps
CONTAINER ID IMAGE COMMAND
CREATED STATUS PORTS NAMES
3e996db98071 registry.access.redhat.com/ubi8/httpd-24:1-163 /usr/bin/run-http...
3 minutes ago Up 3 minutes ago 0.0.0.0:8080->8080/tcp webapp
```

Observe el ID del contenedor. Use esta información para confirmar que `systemd` crea un contenedor cuando reinicia el servicio.

- 7.5. Detenga el servicio `container-webapp` y confirme que el contenedor ya no existe. Cuando detenga el servicio, `systemd` se detiene y, luego, elimina el contenedor.

```
[contsvc@servera user]$ systemctl --user stop container-webapp
[contsvc@servera user]$ podman ps --all
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
```

- 7.6. Inicie el servicio `container-webapp` y, luego, confirme que el contenedor se esté ejecutando.

capítulo 16 | Ejecución de contenedores

El ID del contenedor es diferente, ya que el daemon `systemd` crea un contenedor con la instrucción `start` y elimina el contenedor con la instrucción `stop`.

```
[contsvc@servera user]$ systemctl --user start container-webapp
[contsvc@servera user]$ podman ps
CONTAINER ID  IMAGE                                     COMMAND
CREATED      STATUS          PORTS          NAMES
4584b4df514c  registry.access.redhat.com/ubi8/httpd-24:1-163  /usr/bin/run-http...
6 seconds ago  Up 7 seconds ago  0.0.0.0:8080->8080/tcp  webapp
```

- 8. Asegúrese de que los servicios para el usuario `contsvc` se inicien en el arranque del sistema. Cuando finalice, reinicie la máquina `servera`.

8.1. Ejecute el comando `loginctl enable-linger`.

```
[contsvc@servera user]$ loginctl enable-linger
```

8.2. Confirme que la opción `Linger` esté establecida para el usuario `contsvc`.

```
[contsvc@servera user]$ loginctl show-user contsvc
...output omitted...
Linger=yes
```

8.3. Cambie al usuario `root` y, luego, use el comando `systemctl reboot` para reiniciar `servera`.

```
[contsvc@servera user]$ su -
Password: redhat
Last login: Fri Aug 28 07:43:40 EDT 2020 on pts/0
[root@servera ~]# systemctl reboot
Connection to servera closed by remote host.
Connection to servera closed.
[student@workstation ~]$
```

- 9. Cuando la máquina `servera` vuelva a estar activa, inicie sesión en `servera` con el usuario `contsvc`. Confirme que `systemd` inició el contenedor `webapp` y que el contenido web esté disponible.

9.1. Inicie sesión en `servera` con el usuario `contsvc`.

```
[student@workstation ~]$ ssh contsvc@servera
...output omitted...
```

9.2. Verifique que el contenedor esté ejecutándose.

```
[contsvc@servera ~]$ podman ps
CONTAINER ID  IMAGE                                     COMMAND
CREATED      STATUS          PORTS          NAMES
6c325bf49f84  registry.access.redhat.com/ubi8/httpd-24:1-163  /usr/bin/run-http...
2 minutes ago  Up 2 minutes ago  0.0.0.0:8080->8080/tcp  webapp
```

9.3. Acceda al contenido web.

```
[contsvc@servera ~]$ curl http://localhost:8080
Hello World
```

9.4. Regrese a la máquina `workstation` como el usuario `student`.

```
[contsvc@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$
```

Finalizar

En la máquina `workstation`, ejecute el script `lab finish containers-services` para terminar este ejercicio.

```
[student@workstation ~]$ lab finish containers-services
```

Esto concluye la sección.

► Trabajo de laboratorio

Ejecución de contenedores

En este trabajo de laboratorio, configura un contenedor en su servidor que proporciona un servicio de base de datos MariaDB, almacena su base de datos en un almacenamiento persistente y se inicia automáticamente con el servidor.

Resultados

- Crear contenedores independientes.
- Configurar el redireccionamiento de puertos y el almacenamiento persistente.
- Configurar `systemd` para que los contenedores se inicien cuando se inicia la máquina host.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start containers-review
```

Instrucciones

1. En `serverb`, instale los paquetes de herramientas del contenedor.
2. El registro de imágenes de contenedores en `registry.lab.example.com` almacena la imagen `rhel8/mariadb-103` con varias etiquetas. Use el usuario `podsvc` para enumerar las etiquetas disponibles y observe la etiqueta con el número de versión *más bajo*. Use el usuario `admin` y la contraseña `redhat321` para autenticarse en el registro. Use el archivo `/tmp/registries.conf` como plantilla para la configuración del registro.
3. Con el usuario `podsvc`, cree el directorio `/home/podsvc/db_data`. Configure el directorio para que los contenedores tengan acceso de lectura y escritura.
4. Cree el contenedor independiente `inventorydb`. Use la imagen `rhel8/mariadb-103` del registro `registry.lab.example.com` y especifique la etiqueta con el número de versión más bajo de esa imagen, que encontró en un paso anterior. Asigne el puerto 3306 en el contenedor al puerto 13306 en el host. Monte el directorio `/home/podsvc/db_data` en el host como `/var/lib/mysql/data` en el contenedor. Declare los siguientes valores de variables para el contenedor:

Variable	Valor
MYSQL_USER	operator1
MYSQL_PASSWORD	redhat
MYSQL_DATABASE	inventory
MYSQL_ROOT_PASSWORD	redhat

Puede copiar y pegar estos parámetros desde el archivo `/home/podsvc/containers-review/variables` en `serverb`. Ejecute el script `/home/podsvc/containers-review/testdb.sh` para confirmar que la base de datos de MariaDB se esté ejecutando.

- Configure el daemon `systemd` para que el contenedor `inventorydb` se inicie automáticamente cuando arranque el sistema.

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade containers-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish containers-review
```

Esto concluye la sección.

► Solución

Ejecución de contenedores

En este trabajo de laboratorio, configura un contenedor en su servidor que proporciona un servicio de base de datos MariaDB, almacena su base de datos en un almacenamiento persistente y se inicia automáticamente con el servidor.

Resultados

- Crear contenedores independientes.
- Configurar el redireccionamiento de puertos y el almacenamiento persistente.
- Configurar `systemd` para que los contenedores se inicien cuando se inicia la máquina host.

Antes De Comenzar

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start containers-review
```

Instrucciones

1. En `serverb`, instale los paquetes de herramientas del contenedor.

- 1.1. Inicie sesión en `serverb` con el usuario `student`.

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
[student@serverb ~]$
```

- 1.2. Instale el paquete `container-tools`.

```
[student@serverb ~]$ sudo dnf install container-tools
[sudo] password for student: student
...output omitted...
Is this ok [y/N]: y
...output omitted...
Complete!
```

2. El registro de imágenes de contenedores en `registry.lab.example.com` almacena la imagen `rhel8/mariadb-103` con varias etiquetas. Use el usuario `podsvc` para enumerar las etiquetas disponibles y observe la etiqueta con el número de versión *más bajo*. Use el usuario `admin` y la contraseña `redhat321` para autenticarse en el registro. Use el archivo `/tmp/registries.conf` como plantilla para la configuración del registro.

- 2.1. Regrese a la máquina `workstation` como el usuario `student`.

```
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@workstation ~]$
```

- 2.2. Inicie sesión en `serverb` con el usuario `podsvc`.

```
[student@workstation ~]$ ssh podsvc@serverb
...output omitted...
[podsvc@serverb ~]$
```

- 2.3. Configure el acceso al registro del aula `registry.lab.example.com` en su directorio de inicio. Use el archivo `/tmp/registries.conf` como plantilla.

```
[podsvc@serverb ~]$ mkdir -p ~/.config/containers/
[podsvc@serverb ~]$ cp /tmp/registries.conf \
~/.config/containers/
```

- 2.4. Inicie sesión en el registro de contenedores con el comando `podman login`.

```
[podsvc@serverb ~]$ podman login registry.lab.example.com
Username: admin
Password: redhat321
Login Succeeded!
```

- 2.5. Vea la información acerca de la imagen `registry.lab.example.com/rhel8/mariadb-103`.

```
[podsvc@serverb ~]$ skopeo inspect \
docker://registry.lab.example.com/rhel8/mariadb-103
{
  "Name": "registry.lab.example.com/rhel8/mariadb-103",
  "Digest": "sha256:a95b...4816",
  "RepoTags": [
    "1-86",
    "1-102",
    "latest"
  ],
  ...output omitted...
```

La etiqueta de versión más baja es la versión 1-86.

3. Con el usuario `podsvc`, cree el directorio `/home/podsvc/db_data`. Configure el directorio para que los contenedores tengan acceso de lectura y escritura.

- 3.1. Cree el directorio `/home/podsvc/db_data`.

```
[podsvc@serverb ~]$ mkdir /home/podsvc/db_data
```

- 3.2. Defina el modo de acceso del directorio en 777 para que todos tengan acceso de lectura y escritura.

```
[podsvc@serverb ~]$ chmod 777 /home/podsvc/db_data
```

4. Cree el contenedor independiente `inventorydb`. Use la imagen `rhel8/mariadb-103` del registro `registry.lab.example.com` y especifique la etiqueta con el número de versión más bajo de esa imagen, que encontró en un paso anterior. Asigne el puerto 3306 en el contenedor al puerto 13306 en el host. Monte el directorio `/home/podsvc/db_data` en el host como `/var/lib/mysql/data` en el contenedor. Declare los siguientes valores de variables para el contenedor:

Variable	Valor
<code>MYSQL_USER</code>	<code>operator1</code>
<code>MYSQL_PASSWORD</code>	<code>redhat</code>
<code>MYSQL_DATABASE</code>	<code>inventory</code>
<code>MYSQL_ROOT_PASSWORD</code>	<code>redhat</code>

Puede copiar y pegar estos parámetros desde el archivo `/home/podsvc/containers-review/variables` en `serverb`. Ejecute el script `/home/podsvc/containers-review/testdb.sh` para confirmar que la base de datos de MariaDB se esté ejecutando.

- 4.1. Cree el contenedor.

```
[podsvc@serverb ~]$ podman run -d --name inventorydb -p 13306:3306 \
-e MYSQL_USER=operator1 \
-e MYSQL_PASSWORD=redhat \
-e MYSQL_DATABASE=inventory \
-e MYSQL_ROOT_PASSWORD=redhat \
-v /home/podsvc/db_data:/var/lib/mysql/data:Z \
registry.lab.example.com/rhel8/mariadb-103:1-86
...output omitted...
```

- 4.2. Confirme que la base de datos se esté ejecutando.

```
[podsvc@serverb ~]$ ~/containers-review/testdb.sh
Testing the access to the database...
SUCCESS
```

5. Configure el daemon `systemd` para que el contenedor `inventorydb` se inicie automáticamente cuando arranque el sistema.

- 5.1. Si usó `sudo` o `su` para iniciar sesión con el usuario `podsvc`, salga de `serverb` y use el comando `ssh` para iniciar sesión directamente en `serverb` con el usuario `podsvc`. Recuerde que el daemon `systemd` requiere que el usuario abra una sesión directa desde la consola o a través de SSH. omita este paso si ya inició sesión en la máquina `serverb` con el usuario `podsvc` mediante SSH.

```
[student@workstation ~]$ ssh podsvc@serverb  
...output omitted...  
[podsvc@serverb ~]$
```

5.2. Cree el directorio `~/.config/systemd/user/`.

```
[podsvc@serverb ~]$ mkdir -p ~/.config/systemd/user/
```

5.3. Cree el archivo de unidad `systemd` desde el contenedor en ejecución.

```
[podsvc@serverb ~]$ cd ~/.config/systemd/user/  
[podsvc@serverb user]$ podman generate systemd --name inventorydb --files --new  
/home/podsvc/.config/systemd/user/container-inventorydb.service
```

5.4. Detenga y, luego, elimine el contenedor `inventorydb`.

```
[podsvc@serverb user]$ podman stop inventorydb  
inventorydb  
[podsvc@serverb user]$ podman rm inventorydb  
0d28f0e0a4118ff019691e34afe09b4d28ee526079b58d19f03b324bd04fd545
```

5.5. Indique al daemon `systemd` que vuelva a cargar su configuración y, luego, habilite e inicie el servicio `container-inventorydb`.

```
[podsvc@serverb user]$ systemctl --user daemon-reload  
[podsvc@serverb user]$ systemctl --user enable --now container-inventorydb.service  
Created symlink /home/podsvc/.config/systemd/user/multi-user.target.wants/  
container-inventorydb.service → /home/podsvc/.config/systemd/user/container-  
inventorydb.service.  
Created symlink /home/podsvc/.config/systemd/user/default.target.wants/  
container-inventorydb.service → /home/podsvc/.config/systemd/user/container-  
inventorydb.service.
```

5.6. Confirme que el contenedor se esté ejecutando.

```
[podsvc@serverb user]$ ~/containers-review/testdb.sh  
Testing the access to the database...  
SUCCESS  
[podsvc@serverb user]$ podman ps  
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES  
3ab24e7f000d registry.lab.example.com/rhel8/mariadb-103:1-86 run-mysqld 47  
seconds ago Up 46 seconds ago 0.0.0.0:13306->3306/tcp inventorydb
```

5.7. Ejecute el comando `logindctl enable-linger` para que los servicios de usuario se inicien automáticamente cuando se inicia el servidor.

```
[podsvc@serverb ~]$ logindctl enable-linger
```

5.8. Regrese a la máquina `workstation` como el usuario `student`.

```
[podsvc@serverb ~]$ exit  
logout  
Connection to serverb closed.  
[student@workstation ~]$
```

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade containers-review
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish containers-review
```

Esto concluye la sección.

Resumen

- Los contenedores proporcionan una manera ligera de distribuir y ejecutar una aplicación con sus dependencias para no entrar en conflicto con el software instalado en el host.
- Los contenedores se ejecutan desde imágenes de contenedores que puede descargar desde un registro de contenedor o que puede crear usted mismo.
- Puede usar archivos de contenedor con instrucciones para crear una imagen de contenedor personalizada.
- Podman, provisto por Red Hat Enterprise Linux, ejecuta y administra directamente los contenedores y las imágenes de contenedores en un único host.
- Los contenedores se pueden ejecutar como `root` o como contenedores rootless sin privilegios para una mayor seguridad.
- Puede asignar puertos de red en el host del contenedor para pasar el tráfico a los servicios que se ejecutan en sus contenedores.
- Puede usar variables de entorno para configurar el software en contenedores en el momento de compilación.
- El almacenamiento de contenedores es temporal, pero puede conectar almacenamiento persistente a un contenedor con el contenido de un directorio en el host del contenedor, por ejemplo.
- Puede configurar un archivo de unidad `systemd` para ejecutar automáticamente contenedores cuando se inicia el sistema.

capítulo 17

Revisión exhaustiva

Meta

Revisar tareas de *Seguimiento rápido de RHCSA*.

Objetivos

- Revisar tareas de *Seguimiento rápido de RHCSA*.

Secciones

- Revisión exhaustiva

Trabajos de laboratorio

- Corrección de problemas de arranque y mantenimiento de servidores
- Configuración y administración de sistemas de archivos y almacenamiento
- Configuración y administración de seguridad del servidor
- Ejecución de contenedores

Revisión exhaustiva

Objetivos

Tras finalizar esta sección, usted debería haber revisado y actualizado las habilidades y los conocimientos aprendidos en *Seguimiento rápido de RHCSA*.

Revisión de Seguimiento rápido de RHCSA

Antes de comenzar la revisión exhaustiva de este curso, debe sentirse cómodo con los temas que se abordaron en cada capítulo.

Puede consultar las secciones anteriores del libro de texto para realizar lecturas complementarias.

Capítulo 1, Sistemas de acceso y obtención de soporte

Edite archivos de texto, inicie sesión en el sistema Linux local y remoto, e investigue los métodos de resolución de problemas proporcionados a través de Red Hat Support y Red Hat Insights.

- Crear y editar archivos de texto desde la línea de comandos con el editor vim.
- Configurar una cuenta de usuario para usar autenticación basada en claves para iniciar sesión en sistemas remotos de forma segura y sin una contraseña.
- Describir y usar los recursos clave en el portal de clientes de Red Hat para encontrar información en la documentación y la base de conocimientos de Red Hat.
- Usar Red Hat Insights para analizar los servidores en busca de problemas, corregirlos o resolverlos, y confirmar que la solución haya funcionado.

Capítulo 2, Administrar archivos desde la línea de comandos

Copiar, mover, crear, eliminar y organizar archivos desde la shell Bash.

- Describir cómo Linux organiza los archivos y los propósitos de diversos directorios en la jerarquía del sistema de archivos.
- Hacer que varios nombres de archivo hagan referencia al mismo archivo con enlaces duros y simbólicos (o "blandos").
- Ejecutar con eficiencia los comandos que afectan a muchos archivos mediante el uso de las funciones de coincidencia de patrones de la shell Bash.

Capítulo 3, Administración de usuarios y grupos locales

Crear, administrar y eliminar usuarios y grupos locales, y administrar políticas de contraseña locales.

- Describir el propósito de los usuarios y grupos en un sistema Linux.
- Cambiar a la cuenta de superusuario para administrar un sistema Linux y otorgar a otros usuarios acceso de superusuario a través del comando sudo.
- Crear, modificar y eliminar cuentas de usuario locales.

- Crear, modificar y eliminar cuentas de grupo locales.
- Establecer una política de administración de contraseñas para los usuarios, y bloquear y desbloquear manualmente las cuentas de los usuarios.

Capítulo 4, Control de acceso a los archivos

Configurar los permisos del sistema de archivos Linux en los archivos e interpretar los efectos de seguridad de los distintos parámetros de configuración de permisos.

- Cambiar los permisos y la propiedad de los archivos con las herramientas de línea de comandos.
- Controlar los permisos predeterminados de los archivos creados por los usuarios, explicar el efecto de los permisos especiales y usar permisos especiales y permisos predeterminados para configurar el propietario del grupo de archivos creados en un directorio.

Capítulo 5, Administración de seguridad de SELinux

Proteger y administrar la seguridad del servidor con SELinux.

- Explicar cómo SELinux protege los recursos, cambiar el modo de SELinux actual de un sistema y definir el modo de SELinux predeterminado de un sistema.
- Administrar las reglas de política de SELinux que determinan el contexto predeterminado para archivos y directorios con el comando `semanage fcontext` y aplicar el contexto definido por la política de SELinux a archivos y directorios con el comando `restorecon`.
- Activar y desactivar las reglas de política de SELinux con el comando `setsebool`, administrar el valor persistente de los booleanos de SELinux con el comando `semanage boolean -l` y consultar las páginas `man` que terminan con `_selinux` para encontrar información útil acerca de los booleanos de SELinux.
- Usar las herramientas de análisis de registros de SELinux y visualizar información útil durante la solución de problemas de SELinux con el comando `sealert`.

Capítulo 6, Ajuste del rendimiento del sistema

Evalue y controle procesos, establezca parámetros de ajuste y adapte las prioridades de programación de procesos en un sistema Red Hat Enterprise Linux.

- Usar comandos para finalizar procesos y comunicarse con ellos, definir las características de un proceso daemon y detener sesiones y procesos de usuario.
- Definir el promedio de carga y determinar los procesos del servidor que consumen muchos recursos.
- Optimizar el rendimiento del sistema seleccionando un perfil de ajuste administrado por el daemon.
- Dar o quitar la prioridad a procesos específicos con los comandos `nice` y `renice`.

Capítulo 7, Programación de tareas futuras

Programar tareas para que se ejecuten automáticamente en el futuro

- Programar comandos para que se ejecuten en un horario de repetición con el archivo `crontab` de un usuario.

- Programar comandos para que se ejecuten en un horario de repetición con el archivo crontab y los directorios del sistema.
- Habilitar y deshabilitar los temporizadores de systemd y configurar un temporizador que administre archivos temporales

Capítulo 8, Instalación y actualización de paquetes de software

Descargar, instalar, actualizar y gestionar paquetes de software de Red Hat y repositorios de paquetes DNF.

- Registrar un sistema para su cuenta de Red Hat y asignarle derechos para actualizaciones de software y servicios de soporte mediante Red Hat Subscription Management.
- Buscar, instalar y actualizar paquetes de software con el comando dnf.
- Habilitar y deshabilitar el uso de repositorios DNF de terceros o de Red Hat por un servidor.

Capítulo 9, Administración de almacenamiento básico

Crear y administrar dispositivos de almacenamiento, particiones, sistemas de archivos y espacios de intercambio (swap) desde la línea de comandos.

- Acceder al contenido de sistemas de archivos mediante la adición y la eliminación de sistemas de archivos de la jerarquía de sistemas de archivos.
- Crear particiones de almacenamiento, formatearlas con sistemas de archivos y montarlas para su uso.
- Crear y administrar espacios de intercambio (swap) para complementar la memoria física.

Capítulo 10, Administración de la pila (stack) de almacenamiento

Crear y administrar volúmenes lógicos que contengan sistemas de archivos o espacios de intercambio (swap) desde la línea de comandos.

- Describir los componentes y conceptos del administrador de volúmenes lógicos e implementar el almacenamiento de LVM y mostrar la información de los componentes de LVM.
- Analizar los múltiples componentes de almacenamiento que conforman las capas de la pila (stack) de almacenamiento.

Capítulo 11, Servicios de control y proceso de arranque

Controlar y monitorear los servicios de red, los daemons del sistema y el proceso de arranque con 'systemd'.

- Enumerar los daemons del sistema y los servicios de red iniciados por el servicio systemd y las unidades socket.
- Controlar los daemons del sistema y los servicios de red con systemctl.
- Describir el proceso de arranque de Red Hat Enterprise Linux, configurar el objetivo predeterminado que se usa en el arranque e iniciar un sistema con un objetivo no predeterminado.
- Iniciar sesión en un sistema y cambiar la contraseña de root cuando la actual se haya perdido.

capítulo 17 | Revisión exhaustiva

- Reparar manualmente la configuración del sistema de archivos o problemas de daños que detengan el proceso de arranque.

Capítulo 12, Analizar y almacenar registros

Ubicar e interpretar correctamente registros de eventos del sistema para la resolución de problemas.

- Describir la arquitectura básica de registro que emplea Red Hat Enterprise Linux para registrar eventos
- Interpretar eventos en archivos syslog relevantes a los fines de resolver problemas o revisar el estado del sistema
- Buscar e interpretar entradas en el diario (journal) del sistema para resolver problemas o revisar el estado del sistema
- Configurar el diario (journal) del sistema para resguardar el registro de eventos cuando se reinicia un servidor
- Mantener una sincronización de hora precisa por medio del Protocolo de Tiempo de la Red (NTP) y configurar la zona horaria para garantizar marcas de tiempo correctas para los eventos registrados por el diario (journal) y los registros del sistema.

Capítulo 13, Administración de redes

Configurar las interfaces de red y la configuración en servidores Red Hat Enterprise Linux.

- Probar e inspeccionar la configuración de red actual con las utilidades de la línea de comando.
- Administrar los parámetros de configuración de red con el comando nmcli.
- Modificar la configuración de la red mediante la edición de los archivos de configuración.
- Configurar el nombre de host estático del servidor y su resolución de nombre, y probar los resultados.

Capítulo 14, Acceso al almacenamiento conectado a la red

Acceder al almacenamiento conectado a la red con el protocolo NFS.

- Identificar la información de exportación de NFS, crear un directorio para usar como punto de montaje, montar una exportación de NFS con el comando `mount` o mediante la configuración del archivo `/etc/fstab` y desmonte una exportación de NFS con el comando `umount`.
- Describir los beneficios de usar el servicio de automontaje y las exportaciones de NFS de automontaje mediante el uso de asignaciones directas e indirectas.

Capítulo 15, Administración de la seguridad de redes

Controlar las conexiones de red a los servicios mediante el firewall del sistema.

- Aceptar o rechazar las conexiones de red a los servicios del sistema con reglas de firewalld.

Capítulo 16, Ejecución de contenedores

Obtener, ejecutar y administrar servicios livianos simples como contenedores en un único servidor de Red Hat Enterprise Linux.

- Explicar los conceptos de contenedores y las tecnologías centrales (core) para crear, almacenar y ejecutar contenedores.
- Analizar las herramientas de administración de contenedores para usar registros para almacenar y recuperar imágenes, y para implementar, consultar y acceder a contenedores.
- Proporcionar almacenamiento persistente para los datos del contenedor al compartir el almacenamiento desde el host del contenedor y configurar una red de contenedores.
- Configurar un contenedor como servicio `systemd` y configurar un servicio de contenedor para que se inicie en el momento del arranque.

► Trabajo de laboratorio

Corrección de problemas de arranque y mantenimiento de servidores



nota

Si planea realizar el examen RHCSA, use el siguiente enfoque para aprovechar al máximo las ventajas de esta revisión integral: intente realizar cada trabajo de laboratorio sin ver los botones de soluciones ni consultar el contenido del curso. Use los scripts de calificación para evaluar su progreso a medida que completa cada trabajo de laboratorio.

En esta revisión, soluciona y repara los problemas de arranque y actualiza el objetivo predeterminado del sistema. También programa tareas para que se ejecuten en un cronograma recurrente como un usuario normal.

Resultados

- Diagnosticar problemas y recuperar el sistema del modo de emergencia.
- Cambiar el objetivo predeterminado de `graphical.target` a `multi-user.target`.
- Programar trabajos recurrentes para que se ejecuten como un usuario normal.

Antes De Comenzar

Si no restableció las máquinas `workstation` y `server` al final del último capítulo, guarde el trabajo que desea mantener de ejercicios anteriores de esas máquinas y restablézcalas ahora.

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start rhcsa-comprevew1
```

Especificaciones

- En `workstation`, ejecute el script `/tmp/rhcsa-break1`. Este script causa un problema con el proceso de arranque en `serverb` y luego reinicia la máquina. Solucione la causa y repare el problema de arranque. Cuando se le solicite, use la contraseña `redhat` del usuario `root`.
- En `workstation`, ejecute el script `/tmp/rhcsa-break2`. Este script hace que el objetivo predeterminado cambie del objetivo `multi-user` al objetivo `graphical` en la máquina `serverb` y, luego, reinicie la máquina. En `serverb`, restablezca el objetivo predeterminado para usar el objetivo `multi-user`. La configuración de objetivo predeterminada debe persistir después del reinicio sin intervención manual. Con el usuario `student`, use el comando `sudo` para ejecutar comandos con privilegios. Use `student` como la contraseña cuando se le solicite.

- En **serverb**, programe un trabajo recurrente con el usuario **student** que ejecuta el script **/home/student/backup-home.sh** por hora entre las 7 p. m. y las 9 p. m. todos los días excepto sábados y domingos. Descargue el script de copia de seguridad desde <http://materials.example.com/labs/backup-home.sh>. El script **backup-home.sh** realiza una copia de seguridad del directorio **/home/student** de **serverb** a **servera** en el directorio **/home/student/serverb-backup**. Use el script **backup-home.sh** para programar el trabajo recurrente con el usuario **student**.
- Reinicie la máquina **serverb** y espere a que el arranque finalice antes de calificar.

Evaluación

Con el usuario **student** en la máquina **workstation**, use el comando **lab** para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade rhcsa-compreview1
```

Finalizar

En la máquina **workstation**, cambie al directorio de inicio de usuario **student** y use el comando **lab** para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish rhcsa-compreview1
```

Esto concluye la sección.

► Solución

Corrección de problemas de arranque y mantenimiento de servidores



nota

Si planea realizar el examen RHCSA, use el siguiente enfoque para aprovechar al máximo las ventajas de esta revisión integral: intente realizar cada trabajo de laboratorio sin ver los botones de soluciones ni consultar el contenido del curso. Use los scripts de calificación para evaluar su progreso a medida que completa cada trabajo de laboratorio.

En esta revisión, soluciona y repara los problemas de arranque y actualiza el objetivo predeterminado del sistema. También programa tareas para que se ejecuten en un cronograma recurrente como un usuario normal.

Resultados

- Diagnosticar problemas y recuperar el sistema del modo de emergencia.
- Cambiar el objetivo predeterminado de `graphical.target` a `multi-user.target`.
- Programar trabajos recurrentes para que se ejecuten como un usuario normal.

Antes De Comenzar

Si no restableció las máquinas `workstation` y `server` al final del último capítulo, guarde el trabajo que desea mantener de ejercicios anteriores de esas máquinas y restablézcalas ahora.

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start rhcsa-comprev1
```

1. En `workstation`, ejecute el script `/tmp/rhcsa-break1`.

```
[student@workstation ~]$ sh /tmp/rhcsa-break1
```

2. Una vez que la máquina `serverb` se haya iniciado, acceda a la consola y observe que el proceso de arranque se detuvo antes de tiempo. Tómese un momento para especular sobre la posible causa de este comportamiento.
 - 2.1. Localice el ícono de la consola de `serverb`, según corresponda para el entorno del aula. Abra la consola e inspeccione el error. El error puede tardar unos segundos en aparecer.

- 2.2. Presione **Ctrl+Alt+Del** para reiniciar la máquina **serverb**. Cuando el menú del cargador de arranque aparezca, presione cualquier tecla excepto **Enter** para interrumpir la cuenta regresiva.
- 2.3. Edite la entrada predeterminada del cargador de arranque en la memoria para iniciar sesión en el modo de emergencia. Presione **e** para editar la entrada actual.
- 2.4. Use las teclas de dirección para navegar hacia la línea que comienza con **linux**. Anexe **systemd.unit=emergency.target**.
- 2.5. Presione **Ctrl+x** para arrancar con la configuración modificada.
- 2.6. Inicie sesión en el modo de emergencia. Use **redhat** como contraseña del usuario **root**.

```
Give root password for maintenance
(or press Control-D to continue): redhat
[root@serverb ~]#
```

3. Vuelva a montar el sistema de archivos **/** con capacidades de lectura y escritura. Use el comando **mount -a** para intentar montar todos los demás sistemas de archivos.
 - 3.1. Vuelva a montar el sistema de archivos **/** con capacidades de lectura y escritura para editar el sistema de archivos.

```
[root@serverb ~]# mount -o remount,rw /
```

- 3.2. Intente montar todos los demás sistemas de archivos. Observe que uno de los sistemas de archivos no se puede montar.

```
[root@serverb ~]# mount -a
...output omitted...
mount: /FakeMount: can't find UUID=fake.
```

- 3.3. Edite el archivo **/etc/fstab** para corregir el problema. Elimine o comente la línea incorrecta.

```
[root@serverb ~]# vim /etc/fstab
...output omitted...
#UUID=fake      /FakeMount  xfs    defaults    0 0
```

- 3.4. Actualice el daemon **systemd** para que el sistema registre la nueva configuración del archivo **/etc/fstab**.

```
[root@serverb ~]# systemctl daemon-reload
[ 206.828912] systemd[1]: Reloading.
```

- 3.5. Intente montar todas las entradas para verificar que el archivo **/etc/fstab** ahora sea correcto.

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

- 3.6. Reinicie `serverb` y espere a que el arranque finalice. El sistema ahora debería arrancar sin errores.

```
[root@serverb ~]# systemctl reboot
```

4. En `workstation`, ejecute el script `/tmp/rhcsa-break2`. Espere a que la máquina `serverb` complete el reinicio antes de continuar.

```
[student@workstation ~]$ sh /tmp/rhcsa-break2
```

5. En `serverb`, defina el objetivo `multi-user` como destino actual y predeterminado.

- 5.1. Inicie sesión en `serverb` con el usuario `student`.

```
[student@workstation ~]$ ssh student@serverb  
...output omitted...  
[student@serverb ~]$
```

- 5.2. Determine el objetivo predeterminado.

```
[student@serverb ~]$ systemctl get-default  
graphical.target
```

- 5.3. Cambie al objetivo `multi-user`.

```
[student@serverb ~]$ sudo systemctl isolate multi-user.target  
[sudo] password for student: student
```

- 5.4. Defina el objetivo `multi-user` como objetivo predeterminado.

```
[student@serverb ~]$ sudo systemctl set-default multi-user.target  
Removed /etc/systemd/system/default.target.  
Created symlink /etc/systemd/system/default.target → /usr/lib/systemd/system/  
multi-user.target.
```

- 5.5. Reinicie `serverb` y verifique que el objetivo `multi-user` esté configurado como objetivo predeterminado.

```
[student@serverb ~]$ sudo systemctl reboot  
Connection to serverb closed by remote host.  
Connection to serverb closed.  
[student@workstation ~]$
```

- 5.6. Despues del reinicio del sistema, abra una sesión de SSH en `serverb` con el usuario `student`. Verifique que el objetivo `multi-user` esté configurado como objetivo predeterminado.

```
[student@workstation ~]$ ssh student@serverb  
...output omitted...  
[student@serverb ~]$ systemctl get-default  
multi-user.target
```

6. En **serverb**, programe un trabajo recurrente con el usuario **student** que ejecuta el script **/home/student/backup-home.sh** por hora entre las 7 p. m. y las 9 p. m. todos los días excepto sábados y domingos. Use el script **backup-home.sh** para programar el trabajo recurrente. Descargue el script de copia de seguridad desde <http://materials.example.com/labs/backup-home.sh>.
- 6.1. En **serverb**, descargue el script de copia de seguridad desde <http://materials.example.com/labs/backup-home.sh>. Use **chmod** para hacer que el script de copia de seguridad sea ejecutable.

```
[student@serverb ~]$ wget http://materials.example.com/labs/backup-home.sh
...output omitted...
[student@serverb ~]$ chmod +x backup-home.sh
```

- 6.2. Abra el archivo crontab con el editor de textos predeterminado.

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

- 6.3. Edite el archivo y agregue la siguiente línea:

```
0 19-21 * * Mon-Fri /home/student/backup-home.sh
```

Guarde los cambios y salga del editor.

- 6.4. Use el comando **crontab -l** para enumerar los trabajos recurrentes programados.

```
[student@serverb ~]$ crontab -l
0 19-21 * * Mon-Fri /home/student/backup-home.sh
```

7. Reinicie **serverb** y espere a que el arranque finalice antes de calificar.

```
[student@serverb ~]$ sudo systemctl reboot
[sudo] password for student: student
Connection to serverb closed by remote host.
Connection to serverb closed.
[student@workstation ~]$
```

Evaluación

Con el usuario **student** en la máquina **workstation**, use el comando **lab** para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade rhcsa-comprevew1
```

Finalizar

En la máquina **workstation**, cambie al directorio de inicio de usuario **student** y use el comando **lab** para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish rhcsa-comprevew1
```

Esto concluye la sección.

► Trabajo de laboratorio

Configuración y administración de sistemas de archivos y almacenamiento



nota

Si planea realizar el examen RHCSA, use el siguiente enfoque para aprovechar al máximo las ventajas de esta revisión integral: intente realizar cada trabajo de laboratorio sin ver los botones de soluciones ni consultar el contenido del curso. Use los scripts de calificación para evaluar su progreso a medida que completa cada trabajo de laboratorio.

En esta revisión, creará un volumen lógico, montará un sistema de archivos de red y creará una partición de intercambio (swap) que se activará automáticamente en el arranque. También configure directorios para almacenar archivos temporales.

Resultados

- Crear un volumen lógico.
- Montar un sistema de archivos de red.
- Crear una partición de intercambio (swap) que se active automáticamente en el arranque.
- Configure el directorio para almacenar archivos temporales.

Antes De Comenzar

Si no restableció las máquinas `workstation` y `server` al final del último capítulo, guarde el trabajo que desea mantener de ejercicios anteriores de esas máquinas y restablézcalas ahora.

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start rhcsa-comprevew2
```

Especificaciones

- En `serverb`, configure un nuevo volumen lógico `vol_home` de 1 GiB en un nuevo grupo de volúmenes `extra_storage` de 2 GiB. Use el disco sin particiones `/dev/vdb` para crear la partición.
- Formatee el volumen lógico `vol_home` con el tipo de sistema de archivos XFS y móntelo en `/user-homes` de manera persistente.
- En `serverb`, monte de forma persistente el sistema de archivos de red `/share` que exporta `servera` en el directorio `/local-share`. La máquina `servera` exporta la ruta `servera.lab.example.com:/share`.

- En `serverb`, cree una nueva partición de intercambio (swap) de 512 MiB en el disco `/dev/vdc`. Monte la partición de intercambio (swap) de manera persistente.
- Cree el grupo de usuarios `production`. Cree los usuarios `production1`, `production2`, `production3` y `production4` con el grupo `production` como grupo adicional.
- En `serverb`, configure el directorio `/run/volatile` para almacenar archivos temporales. Si no se accede a los archivos de este directorio durante más de 30 segundos, el sistema los elimina automáticamente. Defina `0700` como los permisos octales para el directorio. Use el archivo `/etc/tmpfiles.d/volatile.conf` para configurar la eliminación basada en el tiempo de los archivos en el directorio `/run/volatile`.

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade rhcsa-comprevew2
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish rhcsa-comprevew2
```

Esto concluye la sección.

► Solución

Configuración y administración de sistemas de archivos y almacenamiento



nota

Si planea realizar el examen RHCSA, use el siguiente enfoque para aprovechar al máximo las ventajas de esta revisión integral: intente realizar cada trabajo de laboratorio sin ver los botones de soluciones ni consultar el contenido del curso. Use los scripts de calificación para evaluar su progreso a medida que completa cada trabajo de laboratorio.

En esta revisión, creará un volumen lógico, montará un sistema de archivos de red y creará una partición de intercambio (swap) que se activará automáticamente en el arranque. También configure directorios para almacenar archivos temporales.

Resultados

- Crear un volumen lógico.
- Montar un sistema de archivos de red.
- Crear una partición de intercambio (swap) que se active automáticamente en el arranque.
- Configure el directorio para almacenar archivos temporales.

Antes De Comenzar

Si no restableció las máquinas `workstation` y `server` al final del último capítulo, guarde el trabajo que desea mantener de ejercicios anteriores de esas máquinas y restablézcalas ahora.

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start rhcsa-comprevew2
```

1. En `serverb`, configure un nuevo volumen lógico `vol_home` de 1 GiB en un nuevo grupo de volúmenes `extra_storage` de 2 GiB. Use el disco sin particiones `/dev/vdb` para crear la partición.
 - 1.1. Inicie sesión en `serverb` como el usuario `student` y cambie al usuario `root`.

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
[student@serverb ~]$ sudo -i
[sudo] password for student: student
[root@serverb ~]#
```

- 1.2. Cree una partición de 2 GiB en el disco /dev/vdb.

```
[root@serverb ~]# parted /dev/vdb mklabel msdos
...output omitted...
[root@serverb ~]# parted /dev/vdb mkpart primary 1GiB 3GiB
...output omitted...
[root@serverb ~]# parted /dev/vdb set 1 lvm on
...output omitted...
```

- 1.3. Declare el dispositivo de bloque /dev/vdb1 como volumen físico.

```
[root@serverb ~]# pvcreate /dev/vdb1
...output omitted...
```

- 1.4. Cree el grupo de volúmenes extra_storage con la partición /dev/vdb1.

```
[root@serverb ~]# vgcreate extra_storage /dev/vdb1
...output omitted...
```

- 1.5. Cree un volumen lógico vol_home de 1 GiB.

```
[root@serverb ~]# lvcreate -L 1GiB -n vol_home extra_storage
...output omitted...
```

2. Formatee el volumen lógico vol_home con el tipo de sistema de archivos XFS y móntelo en /user-homes de manera persistente.

- 2.1. Cree el directorio /user-homes.

```
[root@serverb ~]# mkdir /user-homes
```

- 2.2. Formatee la partición /dev/extrastorage/vol_home con el tipo de sistema de archivos XFS.

```
[root@serverb ~]# mkfs -t xfs /dev/extrastorage/vol_home
...output omitted...
```

- 2.3. Monte la partición /dev/extrastorage/vol_home de manera persistente en el directorio /user-homes. Use el UUID de la partición para la entrada del archivo /etc/fstab.

```
[root@serverb ~]# lsblk -o UUID /dev/extra_storage/vol_home
UUID
988cf149-0667-4733-abca-f80c6ec50ab6
[root@serverb ~]# echo "UUID=988c...0ab6 /user-homes xfs defaults 0 0" \
>> /etc/fstab
[root@serverb ~]# mount /user-homes
```

3. En serverb, monte de forma persistente el sistema de archivos de red /share que exporta servera en el directorio /local-share. La máquina servera exporta la ruta servera.lab.example.com:/share.

- 3.1. Cree el directorio /local-share.

```
[root@serverb ~]# mkdir /local-share
```

- 3.2. Adjunte la entrada correspondiente al archivo /etc/fstab para que monte de manera persistente el sistema de archivos de red servera.lab.example.com:/share.

```
[root@serverb ~]# echo "servera.lab.example.com:/share /local-share \
nfs rw,sync 0 0" >> /etc/fstab
```

- 3.3. Monte el sistema de archivos de red en el directorio /local-share.

```
[root@serverb ~]# mount /local-share
```

4. En serverb, cree una partición de intercambio (swap) de 512 MiB en el disco /dev/vdc. Active y monte de forma persistente la partición de intercambio (swap).

- 4.1. Cree una partición de 512 MiB en el disco /dev/vdc.

```
[root@serverb ~]# parted /dev/vdc mklabel msdos
...output omitted...
[root@serverb ~]# parted /dev/vdc mkpart primary linux-swap 1MiB 513MiB
...output omitted...
```

- 4.2. Cree el espacio de intercambio (swap) en la partición /dev/vdc1.

```
[root@serverb ~]# mkswap /dev/vdc1
...output omitted...
```

- 4.3. Cree una entrada en el archivo /etc/fstab para montar de manera persistente el espacio de intercambio (swap). Use el UUID de la partición para crear la entrada del archivo /etc/fstab. Active el espacio de intercambio (swap).

```
[root@serverb ~]# lsblk -o UUID /dev/vdc1
UUID
cc18ccb6-bd29-48a5-8554-546bf3471b69
[root@serverb ~]# echo "UUID=cc18...1b69 swap swap defaults 0 0" >> /etc/fstab
[root@serverb ~]# swapon -a
```

5. Cree el grupo de usuarios **production**. A continuación, cree los usuarios **production1**, **production2**, **production3** y **production4** con el grupo **production** como grupo adicional.

```
[root@serverb ~]# groupadd production
[root@serverb ~]# for i in 1 2 3 4; do useradd -G production production$i; done
```

6. En **serverb**, configure el directorio **/run/volatile** para almacenar archivos temporales. Si no se accede a los archivos de este directorio durante más de 30 segundos, el sistema los elimina automáticamente. Defina **0700** como los permisos octales para el directorio. Use el archivo **/etc/tmpfiles.d/volatile.conf** para configurar la eliminación basada en el tiempo de los archivos en el directorio **/run/volatile**.

- 6.1. Cree el archivo **/etc/tmpfiles.d/volatile.conf** con el siguiente contenido:

```
d /run/volatile 0700 root root 30s
```

- 6.2. Use el comando **systemd-tmpfiles --create** para crear el directorio **/run/volatile** si no existe.

```
[root@serverb ~]# systemd-tmpfiles --create /etc/tmpfiles.d/volatile.conf
```

- 6.3. Regrese a la máquina **workstation** como el usuario **student**.

```
[student@serverb ~]$ exit
logout
Connection to serverb closed.
```

Evaluación

Con el usuario **student** en la máquina **workstation**, use el comando **lab** para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade rhcsa-comprevew2
```

Finalizar

En la máquina **workstation**, cambie al directorio de inicio de usuario **student** y use el comando **lab** para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish rhcsa-comprevew2
```

Esto concluye la sección.

► Trabajo de laboratorio

Configuración y administración de seguridad del servidor



nota

Si planea realizar el examen RHCSA, use el siguiente enfoque para aprovechar al máximo las ventajas de esta revisión integral: intente realizar cada trabajo de laboratorio sin ver los botones de soluciones ni consultar el contenido del curso. Use los scripts de calificación para evaluar su progreso a medida que completa cada trabajo de laboratorio.

En esta revisión, configurará la autenticación basada en claves de SSH, cambiará la configuración del firewall, ajustará el modo de SELinux y un booleano de SELinux, y solucionará problemas de SELinux.

Resultados

- Configurar la autenticación basada en claves de SSH.
- Configurar parámetros de firewall.
- Ajustar el modo de SELinux y los booleanos de SELinux.
- Solucionar problemas de SELinux.

Antes De Comenzar

Si no restableció las máquinas `workstation` y `server` al final del último capítulo, guarde el trabajo que desea mantener de ejercicios anteriores de esas máquinas y restablézcalas ahora.

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start rhcsa-comprevew3
```

Especificaciones

- En `serverb`, genere un par de claves SSH para el usuario `student`. No proteja la clave privada con una frase de contraseña.
- Configure el usuario `student` en `servera` para que acepte la autenticación de inicio de sesión con el par de claves de SSH que generó en la máquina `serverb`. El usuario `student` en `serverb` debe ser capaz de iniciar sesión en `servera` con SSH sin ingresar una contraseña.
- En `servera`, verifique los permisos del directorio `/user-homes/production5`. A continuación, configure SELinux para que se ejecute en el modo permissive de manera predeterminada.

- En **serverb**, verifique que el directorio `/localhome` no existe. A continuación, configure el directorio de inicio del usuario `production5` para montar el sistema de archivos de red `/user-homes/production5`. La máquina `servera.lab.example.com` exporta el sistema de archivos como el recurso compartido NFS `servera.lab.example.com:/user-homes/production5`. Use el servicio `autofs` para montar el recurso compartido de red. Verifique que el servicio `autofs` cree el directorio `/localhome/production5` con los mismos permisos que en `servera`.
- En **serverb**, ajuste el booleano correspondiente de SELinux para que el usuario `production5` pueda usar el directorio de inicio montado en NFS después de la autenticación basada en claves de SSH. Si se le solicita, use `redhat` como la contraseña para el usuario `production5`.
- En **serverb**, ajuste la configuración del firewall para rechazar todas las solicitudes de conexión de la máquina `servera`. Use la dirección IPv4 `servera (172.25.250.10)` para configurar la regla de firewall.
- En **serverb**, investigue y corrija el problema de falla del servicio web Apache, que escucha en el puerto `30080/TCP` para las conexiones. Ajuste la configuración del firewall según corresponda para que el puerto `30080/TCP` esté abierto para conexiones entrantes.

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade rhcsa-comprevew3
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish rhcsa-comprevew3
```

Esto concluye la sección.

► Solución

Configuración y administración de seguridad del servidor



nota

Si planea realizar el examen RHCSA, use el siguiente enfoque para aprovechar al máximo las ventajas de esta revisión integral: intente realizar cada trabajo de laboratorio sin ver los botones de soluciones ni consultar el contenido del curso. Use los scripts de calificación para evaluar su progreso a medida que completa cada trabajo de laboratorio.

En esta revisión, configurará la autenticación basada en claves de SSH, cambiará la configuración del firewall, ajustará el modo de SELinux y un booleano de SELinux, y solucionará problemas de SELinux.

Resultados

- Configurar la autenticación basada en claves de SSH.
- Configurar parámetros de firewall.
- Ajustar el modo de SELinux y los booleanos de SELinux.
- Solucionar problemas de SELinux.

Antes De Comenzar

Si no restableció las máquinas `workstation` y `server` al final del último capítulo, guarde el trabajo que desea mantener de ejercicios anteriores de esas máquinas y restablézcalas ahora.

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start rhcsa-comprevew3
```

1. En `serverb`, genere un par de claves SSH para el usuario `student`. No proteja la clave privada con una frase de contraseña.

- 1.1. Inicie sesión en `serverb` con el usuario `student`.

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
```

- 1.2. Use el comando `ssh-keygen` para generar un par de claves de SSH. No proteja la clave privada con una frase de contraseña.

```
[student@serverb ~]$ 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.
The key fingerprint is:
SHA256:+ijpGqjEQSGBR80RNchiRTHw/URQksVdHjsHqVBXeYI student@serverb.lab.example.com
The key's randomart image is:
+---[RSA 3072]----+
|+BBX+o*+o..=+.. |
|+.0.oooo .oE+o . |
|.+ . . . .+ .o |
|.. o . o |
|. . .S |
|... . |
|.0. .. |
|o .o o |
|..o.... |
+---[SHA256]-----+
```

2. Configure el usuario **student** en **servera** para que acepte la autenticación de inicio de sesión con el par de claves de SSH que generó en la máquina **serverb**. El usuario **student** en **serverb** debe ser capaz de iniciar sesión en **servera** con SSH sin ingresar una contraseña.
 - 2.1. Envíe la clave pública del par de claves SSH recientemente generado al usuario **student** en la máquina **servera**.

```
[student@serverb ~]$ ssh-copy-id student@servera
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/student/.ssh/id_rsa.pub"
The authenticity of host 'servera (172.25.250.10)' can't be established.
ED25519 key fingerprint is SHA256:shYfoFG0Nnv42pv7j+HG+FISmCAm4Bh5jfjwwSMJbrw.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? 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@servera's password: student

Number of key(s) added: 1

Now try logging in to the machine, with: "ssh 'student@servera'"
and check to make sure that only the key(s) you wanted were added.
```

- 2.2. Verifique que el usuario **student** pueda iniciar sesión en **servera** desde **serverb** sin ingresar una contraseña. No cierre la conexión.

```
[student@serverb ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

3. En servera, verifique los permisos del directorio /user-homes/production5. A continuación, configure SELinux para que se ejecute en el modo permissive de manera predeterminada.

- 3.1. Verifique los permisos del directorio /user-homes/production5.

```
[student@servera ~]$ ls -ld /user-homes/production5
drwx----- 2 production5 production5 62 May  6 05:27 /user-homes/production5
```

- 3.2. Edite el archivo /etc/sysconfig/selinux para establecer el valor del parámetro SELINUX en permissive.

```
[student@servera ~]$ sudo vi /etc/sysconfig/selinux
...output omitted...
#SELINUX=enforcing
SELINUX=permissive
...output omitted...
```

- 3.3. Reinicie el sistema.

```
[student@servera ~]$ sudo systemctl reboot
Connection to servera closed by remote host.
Connection to servera closed.
[student@serverb ~]$
```

4. En serverb, verifique que el directorio /localhome no existe. A continuación, configure el directorio de inicio del usuario production5 para montar el sistema de archivos de red /user-homes/production5. La máquina servera.lab.example.com exporta el sistema de archivos como el recurso compartido NFS servera.lab.example.com:/user-homes/production5. Use el servicio autofs para montar el recurso compartido de red. Verifique que el servicio autofs cree el directorio /localhome/production5 con los mismos permisos que en servera.

- 4.1. Verifique que el directorio /localhome no existe.

```
[student@serverb ~]$ ls -ld /localhome
ls: cannot access '/localhome': No such file or directory
```

- 4.2. En serverb, cambie al usuario root.

```
[student@serverb ~]$ sudo -i
[sudo] password for student: student
[root@serverb ~]#
```

- 4.3. Instale el paquete autofs.

```
[root@serverb ~]# dnf install autofs
...output omitted...
Is this ok [y/N]: y
...output omitted...
Installed:
  autofs-1:5.1.7-27.el9.x86_64      libsss_autofs-2.6.2-2.el9.x86_64

Complete!
```

- 4.4. Cree el archivo de asignación /etc/auto.master.d/production5.autofs con el siguiente contenido:

```
/ - /etc/auto.production5
```

- 4.5. Determine al directorio de inicio del usuario production5.

```
[root@serverb ~]# getent passwd production5
production5:x:5001:5001::/localhome/production5:/bin/bash
```

- 4.6. Cree el archivo /etc/auto.production5 con el siguiente contenido:

```
/localhome/production5 -rw servera.lab.example.com:/user-homes/production5
```

- 4.7. Reinicie el servicio autofs.

```
[root@serverb ~]# systemctl restart autofs
```

- 4.8. Verifique que el servicio autofs cree el directorio /localhome/production5 con los mismos permisos que en servera.

```
[root@serverb ~]# ls -ld /localhome/production5
drwx----- 2 production5 production5 62 May  6 05:52 /localhome/production5
```

5. En serverb, ajuste el booleano correspondiente de SELinux para que el usuario production5 pueda usar el directorio de inicio montado en NFS después de la autenticación basada en claves de SSH. Si se le solicita, use redhat como la contraseña para el usuario production5.

- 5.1. Abra una nueva ventana de terminal y verifique desde servera que el usuario production5 no pueda iniciar sesión en serverb con la autenticación basada en claves SSH. Un booleano de SELinux impide que el usuario inicie sesión. En workstation, abra un nuevo terminal e inicie sesión en servera con el usuario student.

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

- 5.2. Cambie al usuario production5. Cuando se le solicite, use la contraseña redhat del usuario production5.

```
[student@servera ~]$ su - production5
Password: redhat
[production5@servera ~]$
```

5.3. Genere un par de claves SSH.

```
[production5@servera ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/production5/.ssh/id_rsa): Enter
Created directory '/home/production5/.ssh'.
Enter passphrase (empty for no passphrase): Enter
Enter same passphrase again: Enter
Your identification has been saved in /home/production5/.ssh/id_rsa.
Your public key has been saved in /home/production5/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:AbUcIBXneyiGIhr4wS1xz3WqDvbTP+eZuSRn9HQ/cw
    production5@servera.lab.example.com
The key's randomart image is:
+---[RSA 3072]----+
|     ..=++      |
|     . = o      |
|     . . = . . . |
|.. * + o + . . .|
|+= = B S .. o o.|
```

5.4. Transfiera la clave pública del par de claves SSH al usuario **production5** en la máquina **serverb**. Cuando se le solicite, use la contraseña **redhat** del usuario **production5**.

```
[production5@servera ~]$ ssh-copy-id production5@serverb
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/
production5/.ssh/id_rsa.pub"
The authenticity of host 'serverb (172.25.250.11)' can't be established.
ECDSA key fingerprint is SHA256:ciCkaRWF4g6eR9nSdpPxQ7KL8czpViXal6BousK544TY.
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
production5@serverb's password: redhat

Number of key(s) added: 1

Now try logging in to the machine, with: "ssh 'production5@serverb'"
and check to make sure that only the key(s) you wanted were added.
```

- 5.5. Use la autenticación basada en clave pública SSH en lugar de la autenticación basada en contraseña para iniciar sesión en `serverb` con el usuario `production5`. Este comando debería fallar.

```
[production5@servera ~]$ ssh -o pubkeyauthentication=yes \
-o passwordauthentication=no production5@serverb
production5@serverb: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
```

- 5.6. En el terminal que está conectado a `serverb` con el usuario `root`, defina el booleano de SELinux `use_nfs_home_dirs` en `true`.

```
[root@serverb ~]# setsebool -P use_nfs_home_dirs true
```

- 5.7. Vuelva al terminal conectado a `servera` con el usuario `production5` y use la autenticación basada en clave pública SSH en lugar de la autenticación basada en contraseña para iniciar sesión en `serverb` con el usuario `production5`. Este comando debe arrojar resultados satisfactorios.

```
[production5@servera ~]$ ssh -o pubkeyauthentication=yes \
-o passwordauthentication=no production5@serverb
...output omitted...
[production5@serverb ~]$
```

- 5.8. Salga y cierre el terminal que está conectado a `serverb` con el usuario `production5`. Mantenga abierto el terminal que está conectado a `serverb` con el usuario `root`.

6. En `serverb`, ajuste la configuración del firewall para rechazar todas las solicitudes de conexión que se originan de la máquina `servera`. Use la dirección IPv4 `servera` (172.25.250.10) para configurar la regla de firewall.

- 6.1. Agregue la dirección IPv4 de `servera` a la zona `block`.

```
[root@serverb ~]# firewall-cmd --add-source=172.25.250.10/32 \
--zone=block --permanent
success
```

- 6.2. Vuelva a cargar los cambios en la configuración del firewall.

```
[root@serverb ~]# firewall-cmd --reload
success
```

7. En `serverb`, investigue y corrija el problema de falla del servicio web Apache, que escucha en el puerto 30080/TCP para las conexiones. Ajuste la configuración del firewall según corresponda para que el puerto 30080/TCP esté abierto para conexiones entrantes.

- 7.1. Reinicie el servicio `httpd`. Este comando no puede reiniciar el servicio.

```
[root@serverb ~]# systemctl restart httpd.service
Job for httpd.service failed because the control process exited with error code.
See "systemctl status httpd.service" and "journalctl -xeu httpd.service" for
details.
```

capítulo 17 | Revisión exhaustiva

- 7.2. Investigue por qué el servicio `httpd` está fallando. Observe el error de permiso que indica que el daemon `httpd` no pudo vincularse al puerto 30080/TCP en el inicio. Las políticas de SELinux pueden evitar que una aplicación se vincule a un puerto no estándar. Presione `q` para salir del comando.

```
[root@serverb ~]# systemctl status httpd.service
× httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor
   preset: disabled)
     Active: failed (Result: exit-code) since Mon 2022-05-02 13:20:46 EDT; 29s ago
       Docs: man:httpd.service(8)
    Process: 2322 ExecStart=/usr/sbin/httpd $OPTIONS -DFOREGROUND (code=exited,
   status=1/FAILURE)
      Main PID: 2322 (code=exited, status=1/FAILURE)
        Status: "Reading configuration..."
         CPU: 30ms

May 02 13:20:46 serverb.lab.example.com systemd[1]: Starting The Apache HTTP
Server...
May 02 13:20:46 serverb.lab.example.com httpd[2322]: (13)Permission denied:
AH00072: make_sock: could not bind to address [::]:30080
May 02 13:20:46 serverb.lab.example.com httpd[2322]: (13)Permission denied:
AH00072: make_sock: could not bind to address 0.0.0.0:30080
May 02 13:20:46 serverb.lab.example.com httpd[2322]: no listening sockets
available, shutting down
...output omitted...
```

- 7.3. Determine si una política de SELinux está impidiendo que el servicio `httpd` se vincule con el puerto 30080/TCP. El mensaje de registro revela que el puerto 30080/TCP no tiene el contexto apropiado de SELinux `http_port_t`, por lo que SELinux impide que el servicio `httpd` se vincule con el puerto. El mensaje de registro también produce la sintaxis del comando `semanage port` para que pueda corregir fácilmente el problema.

```
[root@serverb ~]# sealert -a /var/log/audit/audit.log
...output omitted...
SELinux is preventing /usr/sbin/httpd from name_bind access on the tcp_socket port
30080.

***** Plugin bind_ports (92.2 confidence) suggests *****

If you want to allow /usr/sbin/httpd to bind to network port 30080
Then you need to modify the port type.
Do
# semanage port -a -t PORT_TYPE -p tcp 30080
  where PORT_TYPE is one of the following: http_cache_port_t, http_port_t,
jboss_management_port_t, jboss.messaging_port_t, ntop_port_t, puppet_port_t.
...output omitted...
```

- 7.4. Defina el contexto apropiado de SELinux en el puerto 30080/TCP para que el servicio `httpd` se vincule con él.

```
[root@serverb ~]# semanage port -a -t http_port_t -p tcp 30080
```

7.5. Reinicie el servicio `httpd`. Este comando debe reiniciar el servicio correctamente.

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

7.6. Agregue el puerto 30080/TCP a la zona `public` predeterminada.

```
[root@serverb ~]# firewall-cmd --add-port=30080/tcp --permanent  
success  
[root@serverb ~]# firewall-cmd --reload  
success
```

7.7. Regrese a la máquina `workstation` como el usuario `student`.

```
[root@serverb ~]# exit  
logout  
[student@serverb ~]$ exit  
logout  
Connection to serverb closed.
```

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade rhcsa-comprevew3
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish rhcsa-comprevew3
```

Esto concluye la sección.

► Trabajo de laboratorio

Ejecución de contenedores



nota

Si planea realizar el examen RHCSA, use el siguiente enfoque para aprovechar al máximo las ventajas de esta revisión integral: intente realizar cada trabajo de laboratorio sin ver los botones de soluciones ni consultar el contenido del curso. Use los scripts de calificación para evaluar su progreso a medida que completa cada trabajo de laboratorio.

Resultados

- Crear contenedores rootless independientes.
- Configurar la asignación de puertos y el almacenamiento persistente.
- Configurar `systemd` para que un contenedor pueda administrarlo con los comandos `systemctl`.

Antes De Comenzar

Si no restableció las máquinas `workstation` y `server` al final del último capítulo, guarde el trabajo que desea mantener de ejercicios anteriores de esas máquinas y restablézcalas ahora.

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start rhcsa-comprevew4
```

Especificaciones

- En `serverb`, configure el usuario `podmgr` con la contraseña `redhat` y configure las herramientas adecuadas para que el usuario `podmgr` administre los contenedores para esta revisión integral. Configure `registry.lab.example.com` como el registro remoto. Use el usuario `admin` y la contraseña `redhat321` para autenticarse. Puede usar el archivo `/tmp/review4/registry.conf` para configurar el registro.
- El directorio `/tmp/review4/container-dev` contiene dos directorios con archivos de desarrollo para los contenedores en esta revisión integral. Copie los dos directorios del directorio `/tmp/review4/container-dev` en el directorio de inicio `podmgr`. Configure el subdirectorio `/home/podmgr/storage/database` para poder usarlo como almacenamiento persistente para un contenedor.
- Cree la red de contenedor habilitada para DNS `production`. Use la subred `10.81.0.0/16` y `10.81.0.1` como puerta de enlace. Use esta red de contenedores para los contenedores que cree en esta revisión integral.

- Cree el contenedor separado db-app01 basado en la imagen de contenedor `registry.lab.example.com/rhel8/mariadb-103` con el número de etiqueta más bajo en la red production. Use el directorio `/home/podmgr/storage/database` como almacenamiento persistente para el directorio `/var/lib/mysql/data` del contenedor db-app01. Asigne el puerto 13306 en la máquina local al puerto 3306 en el contenedor. Use los valores de la siguiente tabla para establecer las variables de entorno para crear la base de datos contenerizada.

Variable	Valor
MYSQL_USER	developer
MYSQL_PASSWORD	redhat
MYSQL_DATABASE	inventory
MYSQL_ROOT_PASSWORD	redhat

- Cree archivos de servicio `systemd` para administrar el contenedor db-app01. Configure el servicio `systemd` para que cuando inicie el servicio, el daemon `systemd` mantenga el contenedor original. Inicie y habilite el contenedor como un servicio `systemd`. Configure el contenedor db-app01 para que se inicien en el arranque del sistema
- Copie el script `/home/podmgr/db-dev/inventory.sql` en el directorio `/tmp` del contenedor db-app01 y ejecútelo dentro del contenedor. Si ejecutó el script de manera local, debería usar el comando `mysql -u root inventory < /tmp/inventory.sql`.
- Use el archivo de contenedor en el directorio `/home/podmgr/http-dev` para crear el contenedor separado http-app01 en la red production. El nombre de la imagen del contenedor debe ser `http-client` con la etiqueta 9.0. Asigne el puerto 8080 en la máquina local al puerto 8080 en el contenedor.
- Use el comando `curl` para consultar el contenido del contenedor http-app01. Verifique que la salida del comando muestre el nombre del contenedor del cliente y que el estado de la base de datos sea up (activo).

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade rhcsa-comprevew4
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish rhcsa-comprevew4
```

Esto concluye la sección.

► Solución

Ejecución de contenedores



nota

Si planea realizar el examen RHCSA, use el siguiente enfoque para aprovechar al máximo las ventajas de esta revisión integral: intente realizar cada trabajo de laboratorio sin ver los botones de soluciones ni consultar el contenido del curso. Use los scripts de calificación para evaluar su progreso a medida que completa cada trabajo de laboratorio.

Resultados

- Crear contenedores rootless independientes.
- Configurar la asignación de puertos y el almacenamiento persistente.
- Configurar `systemd` para que un contenedor pueda administrarlo con los comandos `systemctl`.

Antes De Comenzar

Si no restableció las máquinas `workstation` y `server` al final del último capítulo, guarde el trabajo que desea mantener de ejercicios anteriores de esas máquinas y restablézcalas ahora.

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para preparar el sistema para este ejercicio.

Este comando prepara su entorno y garantiza que estén disponibles todos los recursos requeridos.

```
[student@workstation ~]$ lab start rhcsa-comprevew4
```

1. En `serverb`, configure el usuario `podmgr` con la contraseña `redhat` y configure las herramientas adecuadas para que el usuario `podmgr` administre los contenedores para esta revisión integral. Configure `registry.lab.example.com` como el registro remoto. Use el usuario `admin` y la contraseña `redhat321` para autenticarse. Puede usar el archivo `/tmp/review4/registry.conf` para configurar el registro.
 - 1.1. Inicie sesión en `serverb` con el usuario `student`.

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
[student@serverb ~]$
```

- 1.2. Instale el metapquete `container-tools`.

```
[student@serverb ~]$ sudo dnf install container-tools
[sudo] password for student: student
...output omitted...
Is this ok [y/N]: y
...output omitted...
Complete!
```

- 1.3. Cree el usuario podmgr y defina redhat como contraseña para el usuario.

```
[student@serverb ~]$ sudo useradd podmgr
[student@serverb ~]$ sudo passwd podmgr
Changing password for user podmgr.
New password: redhat
BAD PASSWORD: The password is shorter than 8 characters
Retype new password: redhat
passwd: all authentication tokens updated successfully.
```

- 1.4. Salga de la sesión de usuario student. Inicie sesión en la máquina serverb como el usuario podmgr. Si se le solicita, use redhat como la contraseña.

```
[student@serverb ~]$ exit
logout
Connection to serverb closed.
[student@workstation ~]$ ssh podmgr@serverb
...output omitted...
[podmgr@serverb ~]$
```

- 1.5. Cree el directorio ~/.config/containers.

```
[podmgr@serverb ~]$ mkdir -p ~/.config/containers
```

- 1.6. Copie el archivo /tmp/review4/registries.conf en el directorio de configuración del contenedor en el directorio de inicio.

```
[podmgr@serverb ~]$ cp /tmp/review4/registries.conf ~/.config/containers/
```

- 1.7. Inicie sesión en el registro y compruebe la configuración.

```
[podmgr@serverb ~]$ podman login registry.lab.example.com
Username: admin
Password: redhat321
Login Succeeded!
```

2. El directorio /tmp/review4/container-dev contiene dos directorios con archivos de desarrollo para los contenedores en esta revisión integral. Copie los dos directorios del directorio /tmp/review4/container-dev en el directorio de inicio podmgr. Configure el subdirectorio /home/podmgr/storage/database para poder usarlo como almacenamiento persistente para un contenedor.
- 2.1. Copie el contenido del directorio /tmp/review4/container-dev para el directorio de inicio podmgr.

```
[podmgr@serverb ~]$ cp -r /tmp/review4/container-dev/* .
[podmgr@serverb ~]$ ls -l
total 0
drwxr-xr-x. 2 podmgr podmgr 27 May 10 21:52 db-dev
drwxr-xr-x. 2 podmgr podmgr 44 May 10 21:52 http-dev
```

- 2.2. Cree el directorio `/home/podmgr/storage/database` en el directorio de inicio `podmgr`. Defina los permisos adecuados en el directorio para que el contenedor lo monte como almacenamiento persistente.

```
[podmgr@serverb ~]$ mkdir -p storage/database
[podmgr@serverb ~]$ chmod 0777 storage/database
[podmgr@serverb ~]$ ls -l storage/
total 0
drwxrwxrwx. 2 podmgr podmgr 6 May 10 21:55 database
```

3. Cree la red de contenedor habilitada para DNS `production`. Use la subred `10.81.0.0/16` y `10.81.0.1` como puerta de enlace. Use esta red de contenedores para los contenedores que cree en esta revisión integral.
- 3.1. Cree la red de contenedor habilitada para DNS `production`. Use la subred `10.81.0.0/16` y `10.81.0.1` como puerta de enlace.

```
[podmgr@serverb ~]$ podman network create --gateway 10.81.0.1 \
--subnet 10.81.0.0/16 production
production
```

- 3.2. Verifique que la función DNS esté habilitada en la red `production`.

```
[podmgr@serverb ~]$ podman network inspect production
[
  {
    "name": "production",
    ...output omitted...
    "subnets": [
      {
        "subnet": "10.81.0.0/16",
        "gateway": "10.81.0.1"
      }
    ],
    ...output omitted...
    "dns_enabled": true,
    ...output omitted...
  }
]
```

4. Cree el contenedor separado `db-app01` basado en la imagen de contenedor `registry.lab.example.com/rhel8/mariadb-103` con el número de etiqueta más bajo en la red `production`. Use el directorio `/home/podmgr/storage/database` como almacenamiento persistente para el directorio `/var/lib/mysql/data` del contenedor `db-app01`. Asigne el puerto 13306 en la máquina local al puerto 3306 en el contenedor. Use los valores de la siguiente tabla para establecer las variables de entorno para crear la base de datos contenerizada.

Variable	Valor
MYSQL_USER	developer
MYSQL_PASSWORD	redhat
MYSQL_DATABASE	inventory
MYSQL_ROOT_PASSWORD	redhat

- 4.1. Busque el número de etiqueta de versión más antiguo de la imagen de contenedor `registry.lab.example.com/rhel8/mariadb`.

```
[podmgr@serverb ~]$ skopeo inspect \
docker://registry.lab.example.com/rhel8/mariadb-103
{
  "Name": "registry.lab.example.com/rhel8/mariadb-103",
  "Digest":
  "sha256:a95b678e52bb9f4305cb696e45c91a38c19a7c2c5c360ba6c681b10717394816",
  "RepoTags": [
    "1-86",
    "1-102",
    "latest"
  ...
  .output omitted...
```

- 4.2. Use el número de etiqueta de versión más antiguo de la salida del paso anterior para crear el contenedor separado `db-app01` en la red `production`. Use el directorio `/home/podmgr/storage/database` como almacenamiento persistente para el contenedor. Asigne el puerto 13306 al puerto del contenedor 3306. Use los datos que se proporcionan en la tabla para definir las variables de entorno para el contenedor.

```
[podmgr@serverb ~]$ podman run -d --name db-app01 \
-e MYSQL_USER=developer \
-e MYSQL_PASSWORD=redhat \
-e MYSQL_DATABASE=inventory \
-e MYSQL_ROOT_PASSWORD=redhat \
--network production -p 13306:3306 \
-v /home/podmgr/storage/database:/var/lib/mysql/data:z \
registry.lab.example.com/rhel8/mariadb-103:1-86
...
[podmgr@serverb ~]$ podman ps -a
CONTAINER ID  IMAGE                                     COMMAND      CREATED
           STATUS          PORTS          NAMES
ba398d080e00ba1d52b1cf4f5959c477681cce343c11cc7fc39e4ce5f1cf2384
[podmgr@serverb ~]$
```

CONTAINER ID	IMAGE	COMMAND	CREATED
STATUS	PORTS	NAMES	
ba398d080e00	registry.lab.example.com/rhel8/mariadb-103:1-86	run-mysqld	20 seconds ago
		0.0.0.0:13306->3306/tcp	Up 20 seconds ago
		db-app01	

5. Cree archivos de servicio `systemd` para administrar el contenedor `db-app01`. Configure el servicio `systemd` para que cuando inicie el servicio, el daemon `systemd` mantenga el contenedor original. Inicie y habilite el contenedor como un servicio `systemd`. Configure el contenedor `db-app01` para que se inicien en el arranque del sistema

- 5.1. Cree el directorio `~/.config/systemd/user/` para el archivo de unidad del contenedor.

```
[podmgr@serverb ~]$ mkdir -p ~/.config/systemd/user/
```

- 5.2. Cree el archivo de unidad `systemd` para el contenedor `db-app01` y mueva el archivo de unidad al directorio `~/.config/systemd/user/`.

```
[podmgr@serverb ~]$ podman generate systemd --name db-app01 --files
/home/podmgr/container-db-app01.service
[podmgr@serverb ~]$ mv container-db-app01.service ~/.config/systemd/user/
```

- 5.3. Detenga el contenedor `db-app01`.

```
[podmgr@serverb ~]$ podman stop db-app01
db-app01
[podmgr@serverb ~]$ podman ps -a
CONTAINER ID IMAGE COMMAND CREATED
STATUS PORTS NAMES
ba398d080e00 registry.lab.example.com/rhel8/mariadb-103:1-86 run-mysqld About
an hour ago Exited (0) 3 seconds ago 0.0.0.0:13306->3306/tcp db-app01
```

- 5.4. Vuelva a cargar el servicio del usuario `systemd` para usar la nueva unidad de servicio.

```
[podmgr@serverb ~]$ systemctl --user daemon-reload
```

- 5.5. Inicie y habilite la unidad `systemd` para el contenedor `db-app01`.

```
[podmgr@serverb ~]$ systemctl --user enable --now container-db-app01
Created symlink /home/podmgr/.config/systemd/user/default.target.wants/container-
db-app01.service → /home/podmgr/.config/systemd/user/container-db-app01.service.
[podmgr@serverb ~]$ systemctl --user status container-db-app01
● container-db-app01.service - Podman container-db-app01.service
   Loaded: loaded (/home/podmgr/.config/systemd/user/container-db-app01.service;
   disabled; vendor preset: disabled)
     Active: active (running) since Tue 2022-05-10 22:16:23 EDT; 7s ago
...output omitted...
[podmgr@serverb ~]$ podman ps -a
CONTAINER ID IMAGE COMMAND CREATED
STATUS PORTS NAMES
ba398d080e00 registry.lab.example.com/rhel8/mariadb-103:1-86 run-mysqld 59
seconds ago Up About a minute ago 0.0.0.0:13306->3306/tcp db-app01
```

- 5.6. Use el comando `loginctl` para configurar el contenedor `db-app01` para que se inicie en el arranque del sistema.

```
[podmgr@serverb ~]$ loginctl enable-linger
```

6. Copie el script `/home/podmgr/db-dev/inventory.sql` en el directorio `/tmp` del contenedor `db-app01` y ejecútelo dentro del contenedor. Si ejecutó el script de manera local, debería usar el comando `mysql -u root inventory < /tmp/inventory.sql`.

capítulo 17 | Revisión exhaustiva

- 6.1. Copie el script /home/podmgr/db-dev/inventory.sql en el directorio /tmp del contenedor db-app01.

```
[podmgr@serverb ~]$ podman cp /home/podmgr/db-dev/inventory.sql \
db-app01:/tmp/inventory.sql
```

- 6.2. Ejecute el script inventory.sql en el contenedor db-app01.

```
[podmgr@serverb ~]$ podman exec -it db-app01 sh -c 'mysql -u root inventory
< /tmp/inventory.sql'
```

7. Use el archivo de contenedor en el directorio /home/podmgr/http-dev para crear el contenedor separado http-app01 en la red production. El nombre de la imagen del contenedor debe ser http-client con la etiqueta 9.0. Asigne el puerto 8080 en la máquina local al puerto 8080 en el contenedor.

- 7.1. Cree la imagen http-client:9.0 con el archivo del contenedor en el directorio /home/podmgr/http-dev.

```
[podmgr@serverb ~]$ podman build -t http-client:9.0 http-dev/
STEP 1/7: FROM registry.lab.example.com/rhel8/php-74:1-63
...output omitted...
```

- 7.2. Cree el contenedor independiente http-app01 en la red production. Asigne el puerto 8080 en la máquina local al puerto 8080 en el contenedor.

```
[podmgr@serverb ~]$ podman run -d --name http-app01 \
--network production -p 8080:8080 localhost/http-client:9.0
[podmgr@serverb ~]$ podman ps -a
CONTAINER ID  IMAGE                                     COMMAND      CREATED
           STATUS          PORTS          NAMES
ba398d080e00  registry.lab.example.com/rhel8/mariadb-103:1-86  run-mysqld  20
             minutes ago   Up 20 seconds ago  0.0.0.0:13306->3306/tcp  db-app01
ee424df19621  localhost/http-client:9.0                  /bin/sh -c    4
             seconds ago   Up 4 seconds ago  0.0.0.0:8080->8080/tcp  http-app01
```

8. Consulte el contenido del contenedor http-app01. Verifique que muestre el nombre del contenedor del cliente y que el estado de la base de datos sea up (activo).

- 8.1. Verifique que el contenedor http-app01 responda a solicitudes http.

```
[podmgr@serverb ~]$ curl 127.0.0.1:8080
This is the server http-app01 and the database is up
```

9. Regrese a la máquina workstation como el usuario student.

```
[podmgr@serverb ~]$ exit
logout
Connection to serverb closed.
[student@workstation ~]$
```

Evaluación

Con el usuario `student` en la máquina `workstation`, use el comando `lab` para calificar su trabajo. Corrija los errores informados y vuelva a ejecutar el comando hasta obtener un resultado satisfactorio.

```
[student@workstation ~]$ lab grade rhcsa-comprevew4
```

Finalizar

En la máquina `workstation`, cambie al directorio de inicio de usuario `student` y use el comando `lab` para completar este ejercicio. Este paso es importante para garantizar que los recursos de ejercicios anteriores no impacten en los siguientes.

```
[student@workstation ~]$ lab finish rhcsa-comprevew4
```

Esto concluye la sección.