Red Hat Enterprise Linux 8

Configuración de los ajustes básicos del sistema

Una guía para configurar los ajustes básicos del sistema en Red Hat Enterprise Linux 8

Last Updated: 2021-02-24

Red Hat Enterprise Linux 8 Configuración de los ajustes básicos del sistema

Una guía para configurar los ajustes básicos del sistema en Red Hat Enterprise Linux 8

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

Legal Notice

Resumen

Este documento describe los fundamentos de la administración de sistemas en Red Hat Enterprise Linux 8. El título se centra en: las tareas básicas que un administrador de sistemas necesita hacer justo después de que el sistema operativo haya sido instalado con éxito, la instalación de software con yum, el uso de systemd para la gestión de servicios, la gestión de usuarios, grupos y permisos de archivos, el uso de chrony para configurar NTP, el trabajo con Python 3 y otros.

Table of Contents

HACER QUE EL CÓDIGO ABIERTO SEA MÁS INCLUSIVO

Red Hat se compromete a sustituir el lenguaje problemático en nuestro código, documentación y propiedades web. Estamos empezando con estos cuatro términos: maestro, esclavo, lista negra y lista blanca. Debido a la enormidad de este esfuerzo, estos cambios se implementarán gradualmente a lo largo de varias versiones próximas. Para más detalles, consulte el mensaje de nuestro CTO Chris Wright .

PROPORCIONAR COMENTARIOS SOBRE LA DOCUMENTACIÓN DE RED HAT

Agradecemos su opinión sobre nuestra documentación. Por favor, díganos cómo podemos mejorarla. Para ello:

- Para comentarios sencillos sobre pasajes concretos:
  1. Asegúrese de que está viendo la documentación en el formato *Multi-page HTML*. Además, asegúrese de ver el botón **Feedback** en la esquina superior derecha del documento.
  2. Utilice el cursor del ratón para resaltar la parte del texto que desea comentar.
  3. Haga clic en la ventana emergente **Add Feedback** que aparece debajo del texto resaltado.
  4. Siga las instrucciones mostradas.
- Para enviar comentarios más complejos, cree un ticket de Bugzilla:
  1. Vaya al sitio web de Bugzilla.
  2. Como componente, utilice **Documentation**.
  3. Rellene el campo **Description** con su sugerencia de mejora. Incluya un enlace a la(s) parte(s) pertinente(s) de la documentación.
  4. Haga clic en **Submit Bug**.

CAPÍTULO 1. INTRODUCCIÓN A LA ADMINISTRACIÓN DEL SISTEMA

Las siguientes secciones proporcionan una visión general de las tareas básicas de administración en el sistema instalado.

NOTA

Las siguientes tareas básicas de administración pueden incluir elementos que normalmente se realizan ya durante el proceso de instalación, pero no tienen que hacerse necesariamente, como el registro del sistema. Las secciones que tratan de dichas tareas ofrecen un resumen de cómo puede lograr los mismos objetivos durante la instalación.

Para obtener información sobre la instalación de Red Hat Enterprise Linux, consulte Cómo realizar una instalación estándar de RHEL .

Aunque puede realizar todas las tareas de post-instalación a través de la línea de comandos, también puede utilizar la consola web de RHEL 8 para realizar algunas de ellas.

1.1. CÓMO EMPEZAR A UTILIZAR LA CONSOLA WEB DE RHEL

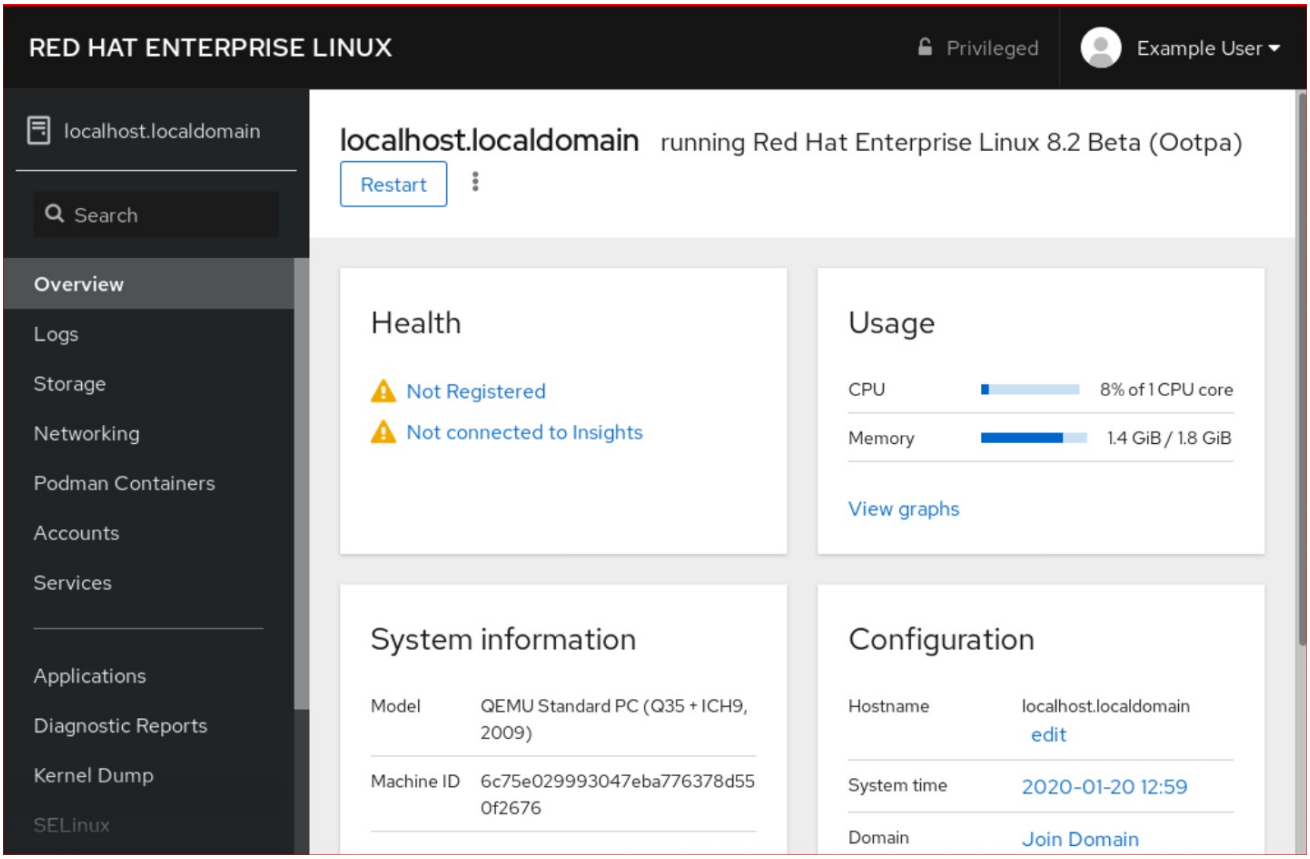
Instale la consola web en Red Hat Enterprise Linux 8 y aprenda a añadir hosts remotos y a supervisarlos en la consola web de RHEL 8.

Requisitos previos

- Instalado Red Hat Enterprise Linux 8.
- Red activada.
- Sistema registrado con la correspondiente suscripción adjunta.
  Para obtener una suscripción, consulte Gestión de suscripciones en la consola web.

1.1.1. ¿Qué es la consola web de RHEL?

La consola web de RHEL es una interfaz basada en la web de Red Hat Enterprise Linux 8 diseñada para gestionar y supervisar su sistema local, así como los servidores Linux ubicados en su entorno de red.



La consola web de RHEL le permite una amplia gama de tareas de administración, incluyendo

- Gestión de servicios
- Gestión de cuentas de usuario
- Gestión y supervisión de los servicios del sistema
- Configuración de las interfaces de red y del cortafuegos
- Revisión de los registros del sistema
- Gestión de máquinas virtuales
- Creación de informes de diagnóstico
- Establecer la configuración del volcado del núcleo
- Configuración de SELinux
- Actualización del software
- Gestión de las suscripciones al sistema

La consola web de RHEL utiliza las mismas APIs del sistema que en un terminal, y las acciones realizadas en un terminal se reflejan inmediatamente en la consola web de RHEL.

Puede supervisar los registros de los sistemas en el entorno de la red, así como su rendimiento, mostrado en forma de gráficos. Además, puedes cambiar la configuración directamente en la consola web o a través del terminal.

1.1.2. Instalación y habilitación de la consola web

Para acceder a la consola web de RHEL 8, primero hay que habilitar el servicio **cockpit.socket**.

Red Hat Enterprise Linux 8 incluye la consola web de RHEL 8 instalada por defecto en muchas variantes de instalación. Si este no es el caso en su sistema, instale el paquete **cockpit** antes de habilitar el servicio **cockpit.socket**.

Procedimiento

1. Si la consola web no está instalada por defecto en su variante de instalación, instale manualmente el paquete **cockpit**:

```
# yum install cockpit
```

2. Habilite e inicie el servicio **cockpit.socket**, que ejecuta un servidor web:

```
# systemctl enable --now cockpit.socket
```

3. Si la consola web no estaba instalada por defecto en su variante de instalación y está utilizando un perfil de cortafuegos personalizado, añada el servicio **cockpit** a **firewalld** para abrir el puerto 9090 en el cortafuegos:

```
# firewall-cmd --add-service=cockpit --permanent
# firewall-cmd --reload
```

Pasos de verificación

1. Para verificar la instalación y configuración anteriores, abra la consola web.

1.1.3. Iniciar sesión en la consola web

Siga los pasos de este procedimiento para acceder por primera vez a la consola web de RHEL utilizando un nombre de usuario y una contraseña del sistema.

Requisitos previos

- Utilice uno de los siguientes navegadores para abrir la consola web:
  - Mozilla Firefox 52 y posteriores
  - Google Chrome 57 y posteriores
  - Microsoft Edge 16 y posteriores
- Credenciales de la cuenta de usuario del sistema
  La consola web de RHEL utiliza una pila PAM específica ubicada en **/etc/pam.d/cockpit**. La autenticación con PAM permite iniciar la sesión con el nombre de usuario y la contraseña de cualquier cuenta local del sistema.

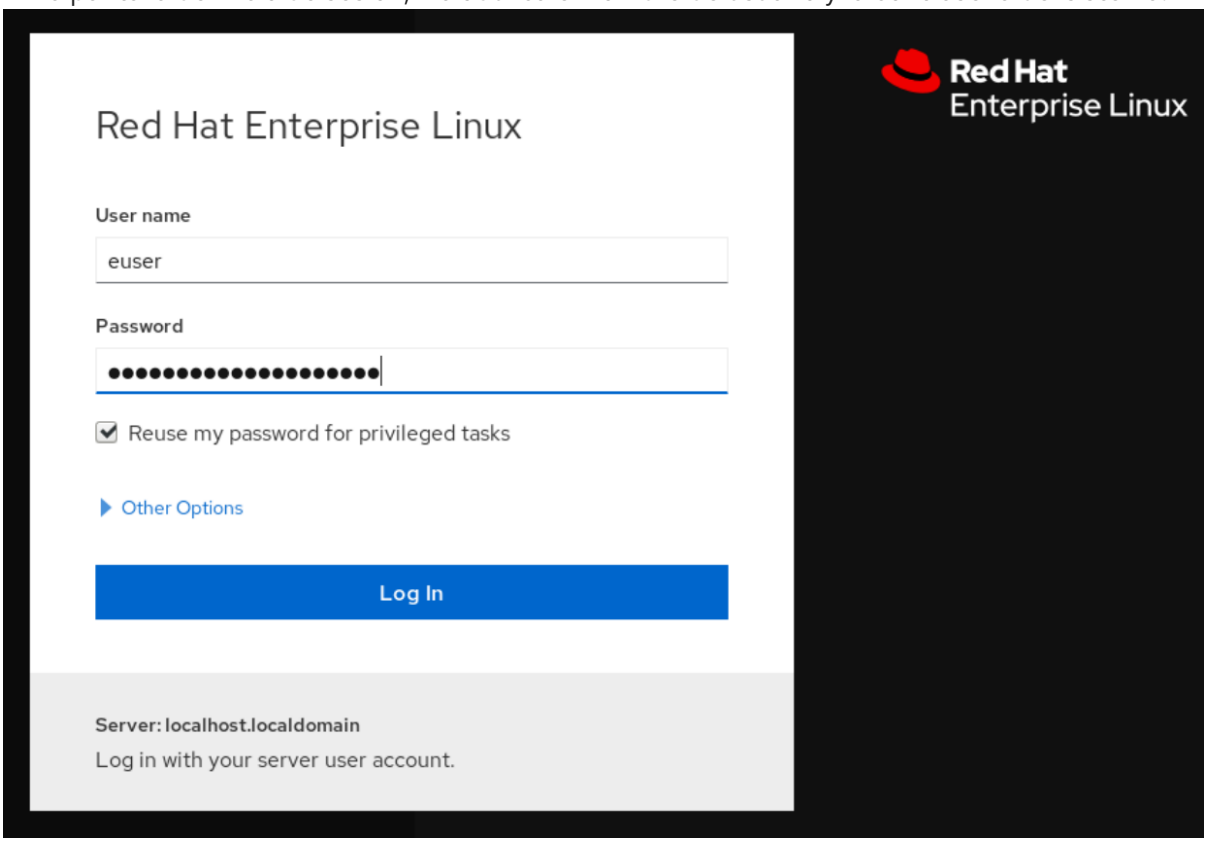
Procedimiento

1. Abra la consola web en su navegador:
   - A nivel local **https://localhost:9090**

- De forma remota con el nombre del servidor **https://example.com:9090**
- De forma remota con la dirección IP del servidor **https://192.0.2.2:9090**
  Si utiliza un certificado autofirmado, el navegador emite una advertencia. Compruebe el certificado y acepte la excepción de seguridad para proceder al inicio de sesión.

  La consola carga un certificado desde el directorio **/etc/cockpit/ws-certs.d** y utiliza el último archivo con extensión **.cert** en orden alfabético. Para evitar tener que conceder excepciones de seguridad, instale un certificado firmado por una autoridad de certificación (CA).

2. En la pantalla de inicio de sesión, introduzca el nombre de usuario y la contraseña del sistema.



3. Opcionalmente, haga clic en la opción **Reuse my password for privileged tasks**
   Si la cuenta de usuario que está utilizando para iniciar la sesión tiene privilegios sudo, esto hace posible realizar tareas privilegiadas en la consola web, como la instalación de software o la configuración de SELinux.

4. Haga clic en **Log In**.

Después de la autenticación exitosa, se abre la interfaz de la consola web de RHEL.

1.1.4. Conexión a la consola web desde una máquina remota

Es posible conectarse a la interfaz de su consola web desde cualquier sistema operativo cliente y también desde teléfonos móviles o tabletas.

Requisitos previos

- Dispositivo con un navegador de Internet compatible, como:
  - Mozilla Firefox 52 y posteriores

- Google Chrome 57 y posteriores
- Microsoft Edge 16 y posteriores

- El servidor RHEL 8 al que desea acceder con una consola web instalada y accesible. Para obtener más información sobre la instalación de la consola web, consulte Instalación de la consola web.

Procedimiento

1. Abra su navegador web.
2. Escriba la dirección del servidor remoto en uno de los siguientes formatos:
   a. Con el nombre del servidor **server.hostname.example.com:port_number**
   b. Con la dirección IP del servidor **server.IP_address:port_number**
3. Después de que se abra la interfaz de acceso, inicie la sesión con las credenciales de su máquina RHEL.

1.1.5. Iniciar sesión en la consola web con una contraseña de un solo uso

Si su sistema forma parte de un dominio de gestión de identidades (IdM) con una configuración de contraseña de un solo uso (OTP) habilitada, puede utilizar una OTP para iniciar sesión en la consola web de RHEL.

IMPORTANTE

Es posible iniciar la sesión con una contraseña de un solo uso sólo si su sistema forma parte de un dominio de Gestión de Identidades (IdM) con la configuración de OTP activada. Para obtener más información sobre OTP en IdM, consulte Contraseña de un solo uso en la gestión de identidades.

Requisitos previos

- Se ha instalado la consola web de RHEL.
  Para más detalles, véase Instalación de la consola web .
- Un servidor de gestión de identidades con la configuración OTP activada.
  Para más detalles, véase Contraseña única en Gestión de identidades .
- Un dispositivo de hardware o software configurado que genera tokens OTP.

Procedimiento

1. Abra la consola web de RHEL en su navegador:
   - A nivel local **https://localhost:PORT_NUMBER**
   - De forma remota con el nombre del servidor **https://example.com:PORT_NUMBER**
   - De forma remota con la dirección IP del servidor
     https://EXAMPLE.SERVER.IP.ADDR:PORT_NUMBER
     Si utiliza un certificado autofirmado, el navegador emite una advertencia. Compruebe el certificado y acepte la excepción de seguridad para proceder al inicio de sesión.

La consola carga un certificado desde el directorio **/etc/cockpit/ws-certs.d** y utiliza el último archivo con extensión **.cert** en orden alfabético. Para evitar tener que conceder excepciones de seguridad, instale un certificado firmado por una autoridad de certificación (CA).

2. Se abre la ventana de inicio de sesión. En la ventana de inicio de sesión, introduzca el nombre de usuario y la contraseña del sistema.
3. Genere una contraseña de un solo uso en su dispositivo.
4. Introduzca la contraseña de un solo uso en un nuevo campo que aparece en la interfaz de la consola web después de confirmar la contraseña.
5. Haga clic en **Log in**.
6. Al iniciar la sesión con éxito, se accede a la página **Overview** de la interfaz de la consola web.

1.1.6. Reiniciar el sistema mediante la consola web

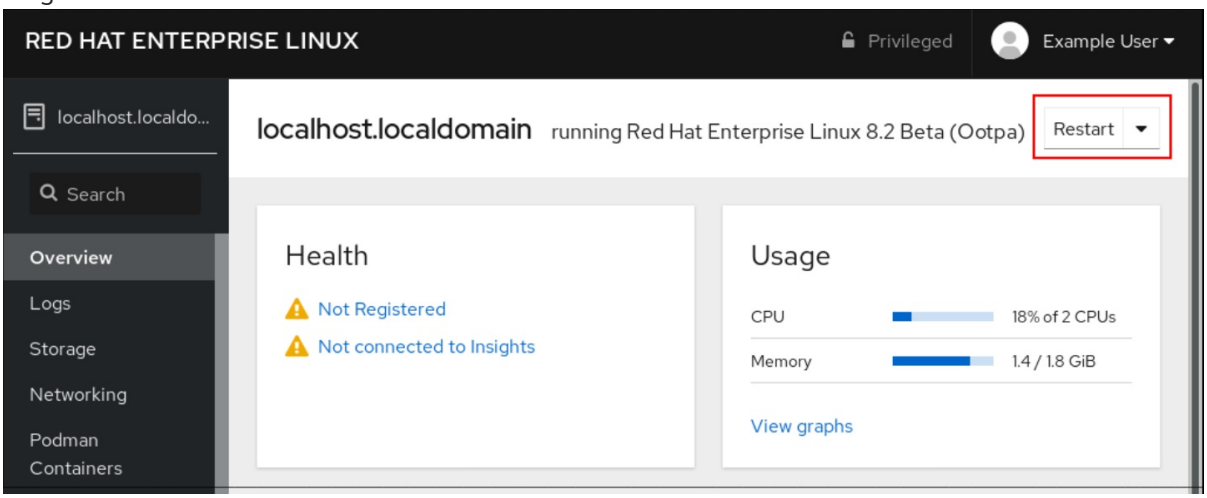
Puede utilizar la consola web para reiniciar un sistema RHEL al que esté conectada la consola web.

Requisitos previos

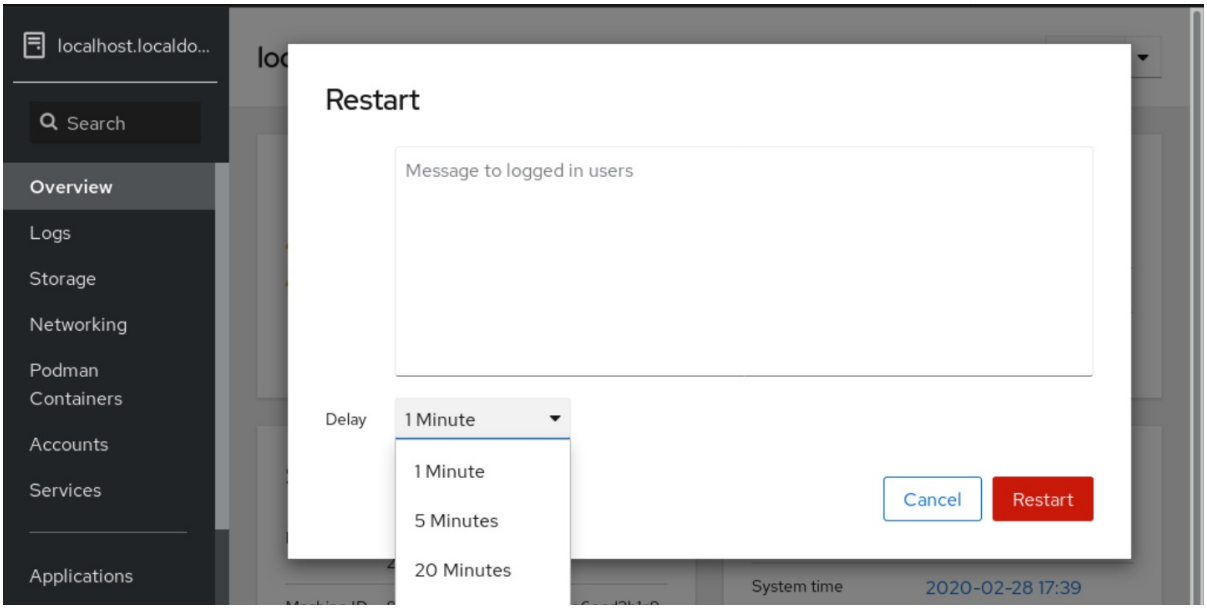
- La consola web está instalada y accesible.
  Para más detalles, véase Instalación de la consola web .

Procedimiento

1. Inicie sesión en la consola web de RHEL 8.
   Para más detalles, consulte Iniciar sesión en la consola web .
2. Haga clic en **Overview**.
3. Haga clic en el botón de reinicio **Restart**.



4. Si hay usuarios registrados en el sistema, escriba una razón para el reinicio en el cuadro de diálogo **Restart**.
5. Opcional: En la lista desplegable **Delay**, seleccione un intervalo de tiempo.



6. Haga clic en **Restart**.

1.1.7. Apagar el sistema mediante la consola web

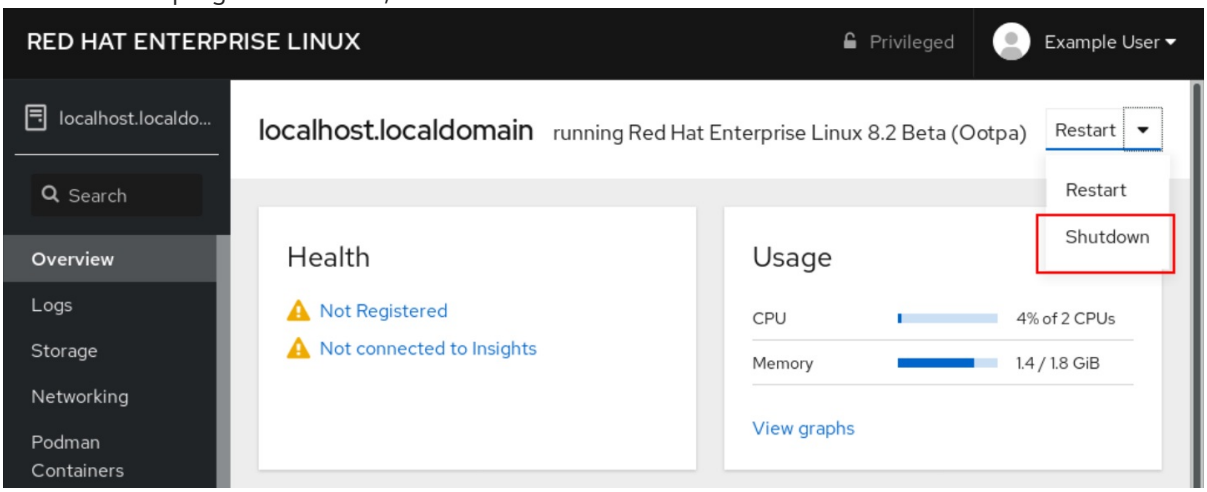
Puede utilizar la consola web para apagar un sistema RHEL al que esté conectada la consola web.

Requisitos previos

- La consola web está instalada y accesible.
  Para más detalles, véase Instalación de la consola web .

Procedimiento

1. Inicie sesión en la consola web de RHEL 8.
   Para más detalles, consulte Iniciar sesión en la consola web .
2. Haga clic en **Overview**.
3. En la lista desplegable **Restart**, seleccione **Shut Down**.



4. Si hay usuarios conectados al sistema, escriba una razón para el cierre en el cuadro de diálogo **Shut Down**.
5. Opcional: En la lista desplegable **Delay**, seleccione un intervalo de tiempo.

6. Haga clic en **Shut Down**.

1.1.8. Configuración de los ajustes de la hora mediante la consola web

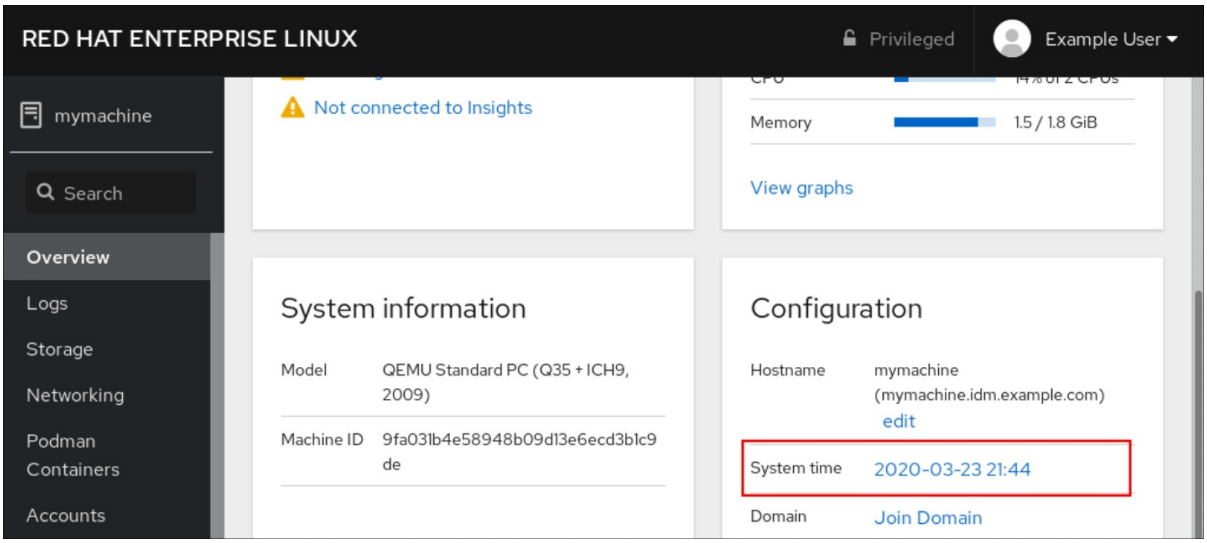
Puede establecer una zona horaria y sincronizar la hora del sistema con un servidor de Protocolo de Tiempo de Red (NTP).

Requisitos previos

- La consola web está instalada y accesible.
  Para más detalles, véase Instalación de la consola web .

Procedimiento

1. Inicie sesión en la consola web de RHEL 8.
   Para más detalles, consulte Iniciar sesión en la consola web .
2. Pulse la hora actual del sistema en **Overview**.



3. En el cuadro de diálogo **Change System Time**, cambie la zona horaria si es necesario.
4. En el menú desplegable **Set Time**, seleccione una de las siguientes opciones:

   Manualmente

   Utilice esta opción si necesita ajustar la hora manualmente, sin un servidor NTP.

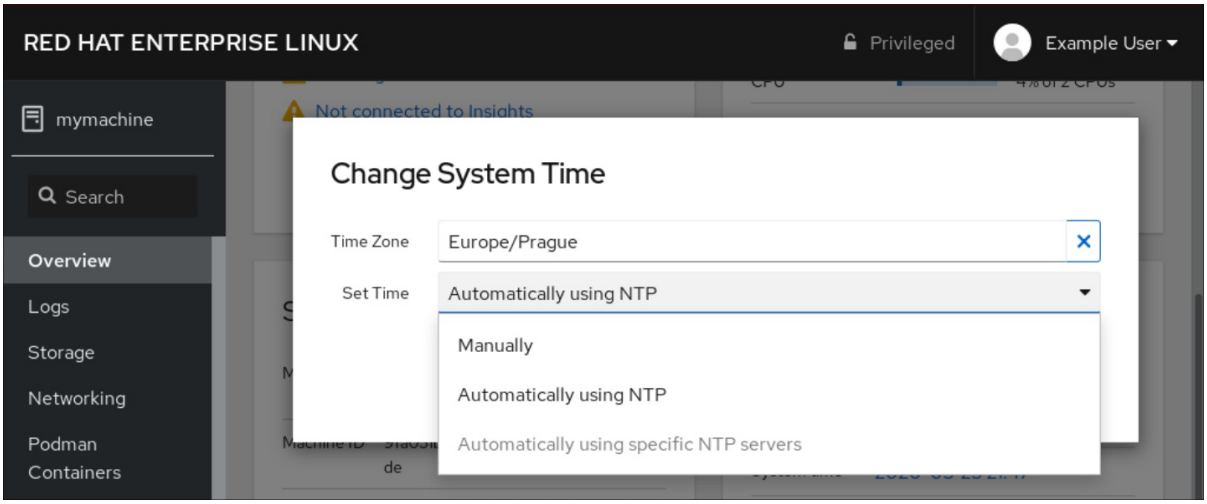
   Uso automático del servidor NTP

   Esta es una opción por defecto, que sincroniza la hora automáticamente con los servidores NTP preestablecidos.

   Uso automático de servidores NTP específicos

   Utilice esta opción sólo si necesita sincronizar el sistema con un servidor NTP específico. Especifique el nombre DNS o la dirección IP del servidor.

5. Haga clic en **Change**.



Pasos de verificación

- Compruebe la hora del sistema que aparece en la pestaña **System**.

Recursos adicionales

- Uso de la suite Chrony para configurar NTP .

1.1.9. Cómo unir un sistema RHEL 8 a un dominio IdM mediante la consola web

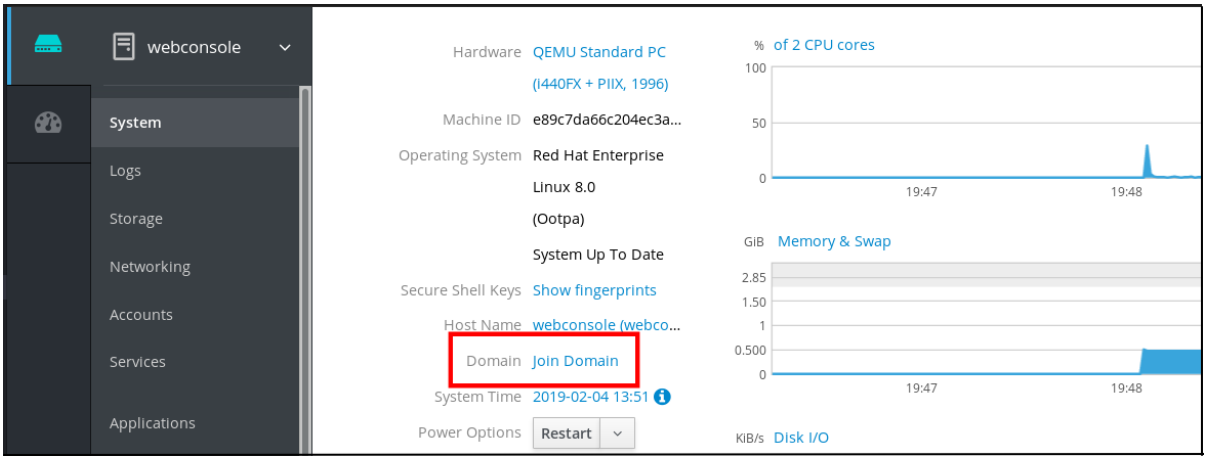
Puede utilizar la consola web para unir el sistema Red Hat Enterprise Linux 8 al dominio de gestión de identidades (IdM).

Requisitos previos

- El dominio IdM está funcionando y es accesible desde el cliente al que se quiere unir.
- Tienes las credenciales de administrador del dominio IdM.

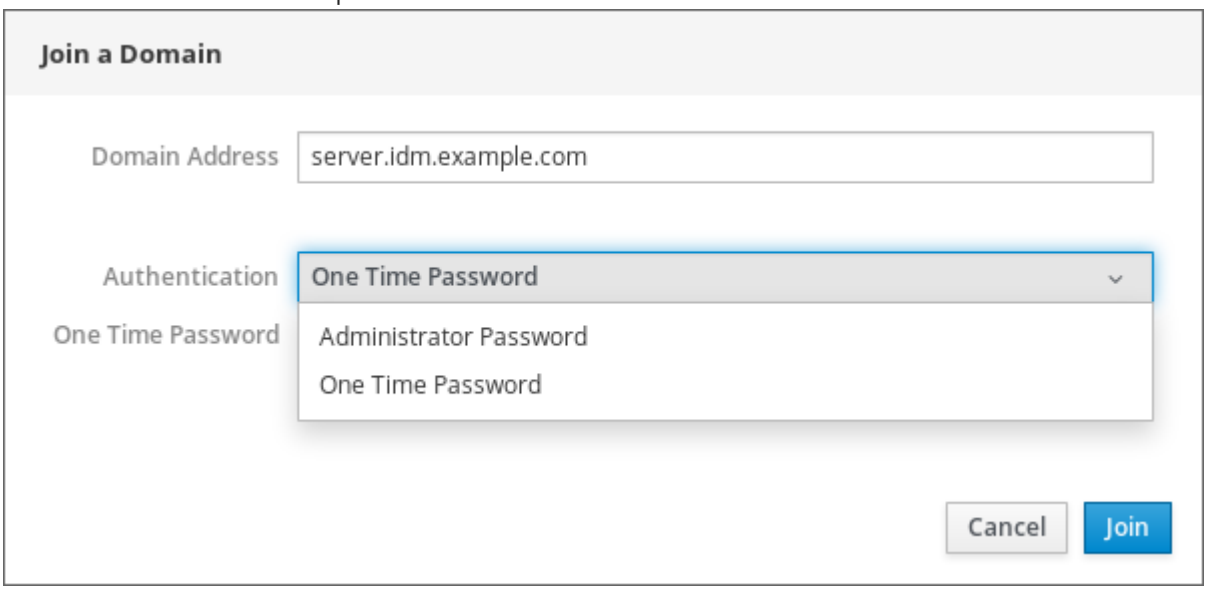
Procedimiento

1. Inicie sesión en la consola web de RHEL.
   Para más detalles, consulte Iniciar sesión en la consola web .
2. Abra la pestaña **System**.
3. Haga clic en **Unirse al dominio**.



4. En el cuadro de diálogo **Join a Domain**, introduzca el nombre del servidor IdM en el campo **Domain Address**.

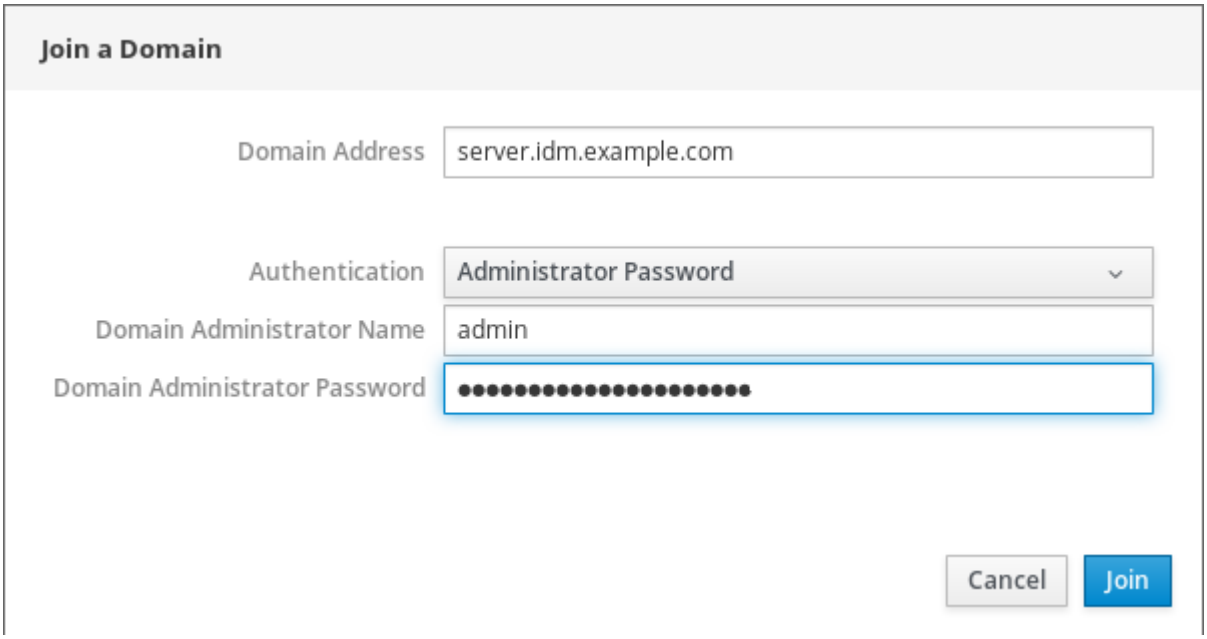
5. En la lista desplegable **Authentication**, seleccione si desea utilizar una contraseña o una contraseña de un solo uso para la autenticación.



6. En el campo **Domain Administrator Name**, introduzca el nombre de usuario de la cuenta de administración de IdM.

7. En el campo de la contraseña, añada la contraseña o la contraseña de un solo uso según lo que haya seleccionado antes en la lista desplegable **Authentication**.

8. Haz clic en **"Únete"**.



Pasos de verificación

1. Si la consola web de RHEL 8 no muestra ningún error, el sistema se ha unido al dominio IdM y puede ver el nombre del dominio en la pantalla **System**.

2. Para verificar que el usuario es miembro del dominio, haga clic en la página Terminal y escriba el comando **id**:

```
$ id
euid=548800004(example_user) gid=548800004(example_user)
groups=548800004(example_user) context=unconfined_u:unconfined_r:unconfined_t:s0-
s0:c0.c1023
```

Recursos adicionales

- Planificación de la gestión de la identidad
- Instalación de la gestión de identidades
- Configurar y gestionar la gestión de identidades

1.1.10. Desactivación de SMT para evitar problemas de seguridad de la CPU mediante la consola web

Desactivar el Multi Threading Simultáneo (SMT) en caso de ataques que abusen del SMT de la CPU. Desactivar SMT puede mitigar las vulnerabilidades de seguridad, como L1TF o MDS.

IMPORTANTE

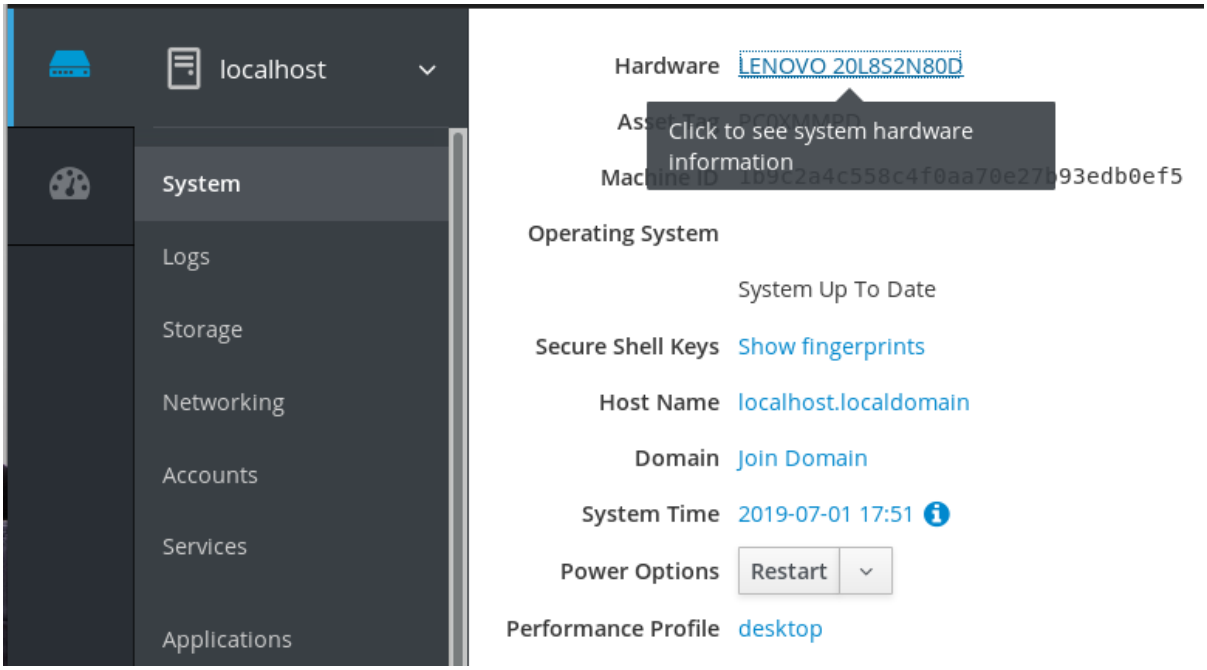
Desactivar el SMT puede reducir el rendimiento del sistema.

Requisitos previos

- La consola web debe estar instalada y accesible.
  Para más detalles, véase Instalación de la consola web .

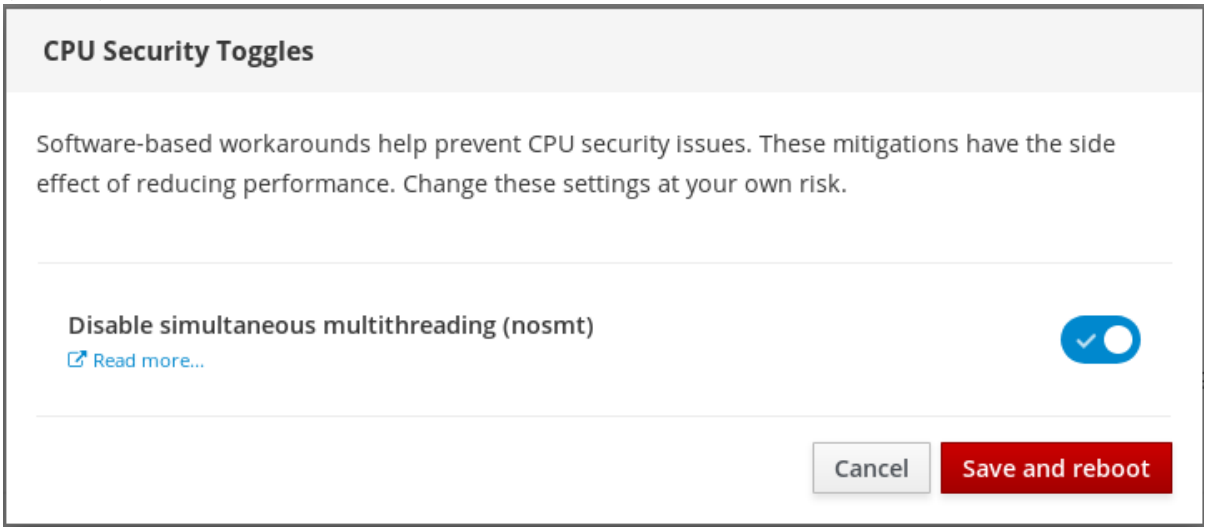
Procedimiento

1. Inicie sesión en la consola web de RHEL 8.
   Para más detalles, consulte Iniciar sesión en la consola web .
2. Haga clic en **System**.
3. En el elemento **Hardware**, haga clic en la información sobre el hardware.



4. En el elemento **CPU Security**, haga clic en **Mitigations**.
Si este enlace no está presente, significa que su sistema no soporta SMT, y por lo tanto no es vulnerable.

5. En la página **CPU Security Toggles**, active la opción **Disable simultaneous multithreading (nosmt)**.



6. Haga clic en el botón **Save and reboot**

Tras el reinicio del sistema, la CPU deja de utilizar el SMT.

Recursos adicionales

- L1TF - Ataque de fallo del terminal L1 - CVE-2018-3620 & CVE-2018-3646
- MDS - Muestreo de datos de microarquitectura - CVE-2018-12130, CVE-2018-12126, CVE-2018-12127 y CVE-2019-11091

1.1.11. Añadir un banner a la página de inicio de sesión

A veces, las empresas o los organismos necesitan mostrar una advertencia de que el uso del ordenador

es para fines legales, que el usuario está sujeto a vigilancia y que se perseguirá a quien lo traspase. La advertencia debe ser visible antes de iniciar la sesión. De manera similar a SSH, la consola web puede mostrar opcionalmente el contenido de un archivo de banner en la pantalla de inicio de sesión. Para habilitar los banners en las sesiones de la consola web, es necesario modificar el archivo **/etc/cockpit/cockpit.conf**. Tenga en cuenta que el archivo no es necesario y puede que tenga que crearlo manualmente.

Requisitos previos

- La consola web está instalada y accesible. Para más detalles, consulte Instalación de la consola web.
- Debes tener privilegios de sudo.

Procedimiento

1. Cree el archivo **/etc/issue.cockpit** en un editor de texto de su preferencia si aún no lo tiene. Añade al archivo el contenido que quieres mostrar como banner.
   No incluya ninguna macro en el archivo, ya que no se realiza ningún reformateo entre el contenido del archivo y el contenido visualizado. Utilice los saltos de línea previstos. Es posible utilizar el arte ASCII.
2. Guarda el archivo.
3. Abra o cree el archivo **cockpit.conf** en el directorio **/etc/cockpit/** en un editor de texto de su preferencia.

```
$ sudo vi cockpit.conf
```

4. Añade el siguiente texto al archivo:

```
[Session]
Banner=/etc/issue.cockpit
```

5. Guarda el archivo.
6. Reinicie la consola web para que los cambios surtan efecto.

```
# systemctl try-restart cockpit
```

Pasos de verificación

- Vuelva a abrir la pantalla de inicio de sesión de la consola web para comprobar que el banner es ahora visible.

Ejemplo 1.1. Añadir un banner de ejemplo a la página de inicio de sesión

1. Cree un archivo **/etc/issue.cockpit** con el texto deseado utilizando un editor de texto:

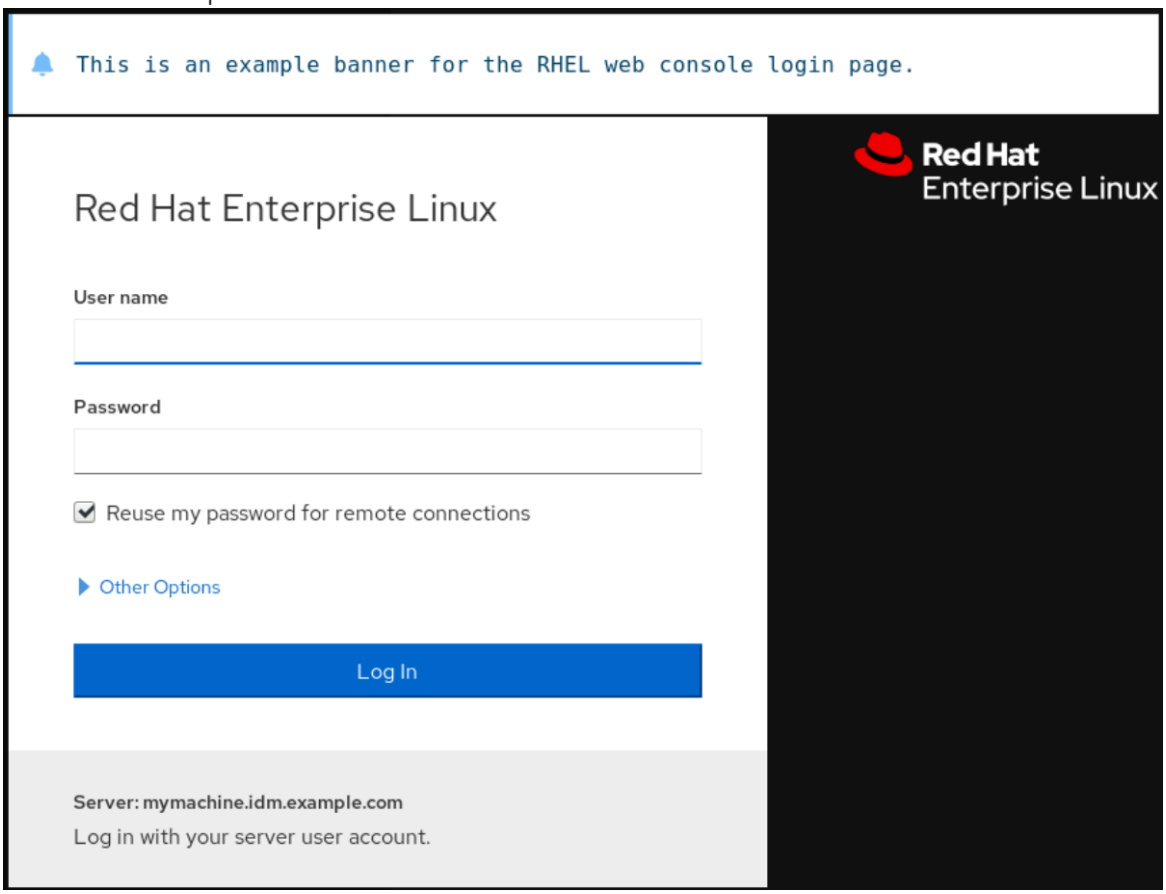
```
Este es un ejemplo de banner para la página de inicio de sesión de la consola web de RHEL.
```

2. Abra o cree el archivo **/etc/cockpit/cockpit.conf** y añada el siguiente texto:

```
[Session]
Banner=/etc/issue.cockpit
```

3. Reinicie la consola web.

4. Vuelva a abrir la pantalla de inicio de sesión de la consola web.



1.1.12. Configuración del bloqueo automático de inactividad en la consola web

Por defecto, no hay ningún tiempo de espera establecido en la interfaz de la consola web. Si desea habilitar un tiempo de espera en su sistema, puede hacerlo modificando el archivo de configuración **/etc/cockpit/cockpit.conf**. Tenga en cuenta que el archivo no es necesario y puede que tenga que crearlo manualmente.

Requisitos previos

- La consola web debe estar instalada y accesible.
  Para más detalles, véase Instalación de la consola web .
- Debes tener privilegios de sudo.

Procedimiento

1. Abra o cree el archivo **cockpit.conf** en el directorio **/etc/cockpit/** en un editor de texto de su preferencia.

```
$ sudo vi cockpit.conf
```

2. Añade el siguiente texto al archivo:

```
[Session]
IdleTimeout=X
```

Sustituya **X** por un número para un período de tiempo de su elección en minutos.

3. Guarda el archivo.

4. Reinicie la consola web para que los cambios surtan efecto.

```
# systemctl try-restart cockpit
```

Pasos de verificación

- Comprueba si la sesión se cierra después de un periodo de tiempo determinado.

1.2. CONFIGURAR EL NOMBRE DE HOST EN LA CONSOLA WEB

Aprenda a utilizar la consola web de RHEL 8 para configurar diferentes formas del nombre del host en el sistema al que está conectada la consola web.

1.2.1. Nombre del anfitrión

El nombre de host identifica el sistema. Por defecto, el nombre de host se establece en **localhost**, pero puede cambiarlo.

Un nombre de host consta de dos partes:

Nombre del anfitrión

Es un nombre único que identifica a un sistema.

Dominio

Añade el dominio como sufijo detrás del nombre de host cuando utilices un sistema en una red y cuando uses nombres en lugar de sólo direcciones IP.

Un nombre de host con un nombre de dominio adjunto se denomina nombre de dominio completo (FQDN). Por ejemplo: **mymachine.example.com**.

Los nombres de los hosts se almacenan en el archivo **/etc/hostname**.

1.2.2. Nombre de host bonito en la consola web

Puede configurar un nombre de host bonito en la consola web de RHEL. El nombre de host bonito es un nombre de host con letras mayúsculas, espacios, etc.

El nombre bonito del host se muestra en la consola web, pero no tiene por qué corresponder con el nombre del host.

Ejemplo 1.2. Formatos de nombres de host en la consola web

Nombre de host bonito

My Machine

Nombre del anfitrión

mymachine

Nombre de host real - nombre de dominio completo (FQDN)

mymachine.idm.company.com

1.2.3. Configurar el nombre del host mediante la consola web

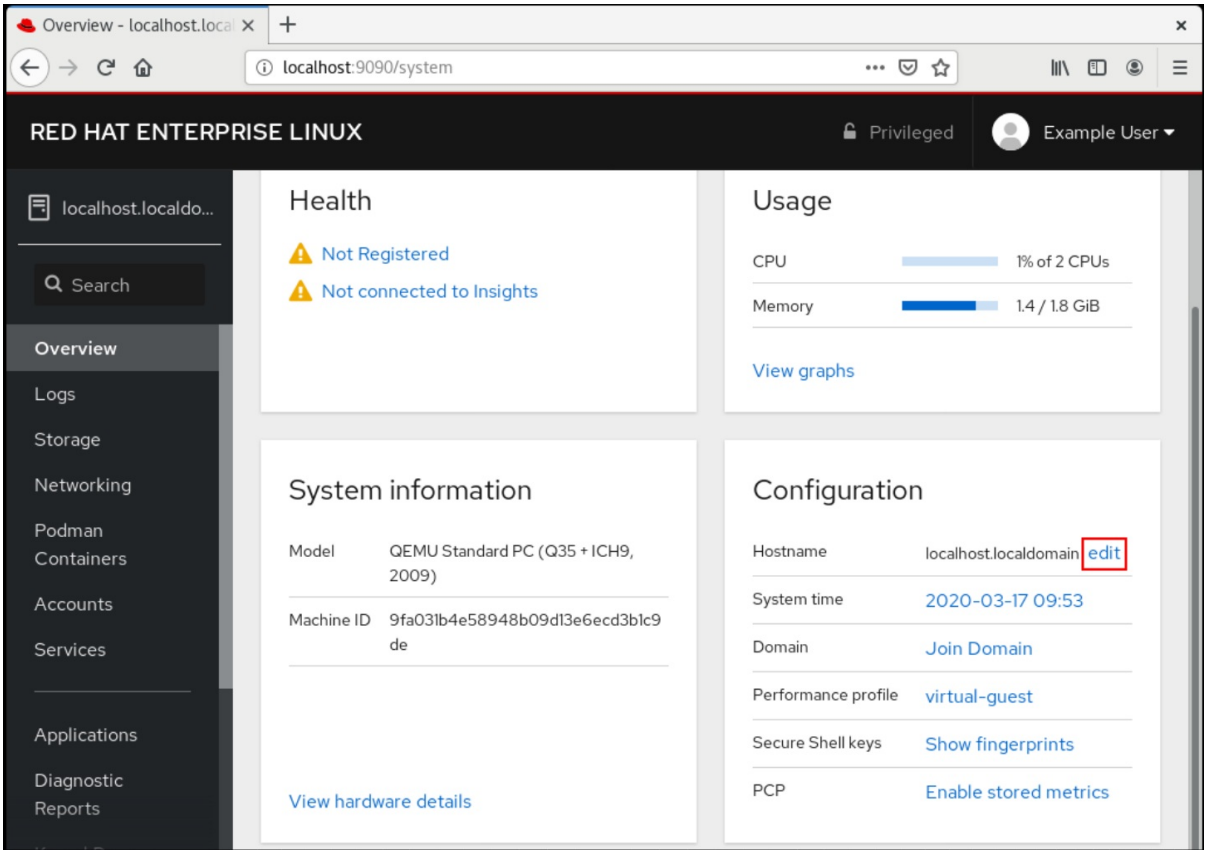
Este procedimiento establece el nombre de host real o el nombre de host bonito en la consola web.

Requisitos previos

- La consola web está instalada y accesible.
  Para más detalles, véase Instalación de la consola web .

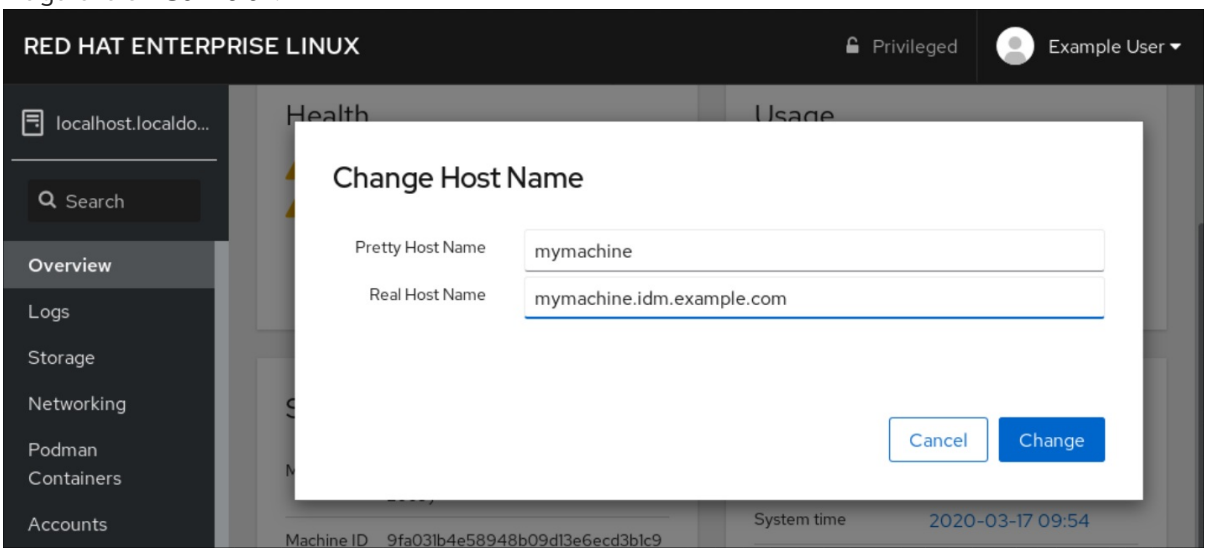
Procedimiento

1. Inicie sesión en la consola web de RHEL 8.
   Para más detalles, consulte Iniciar sesión en la consola web .
2. Haga clic en **"Vista general"**.
3. Haga clic en **editar** junto al nombre del host actual.



4. En el cuadro de diálogo **Change Host Name**, introduzca el nombre del host en el campo **Pretty Host Name**.
5. El campo **Real Host Name** adjunta un nombre de dominio al nombre bonito.
   Puedes cambiar el nombre real del host manualmente si no se corresponde con el nombre bonito del host.

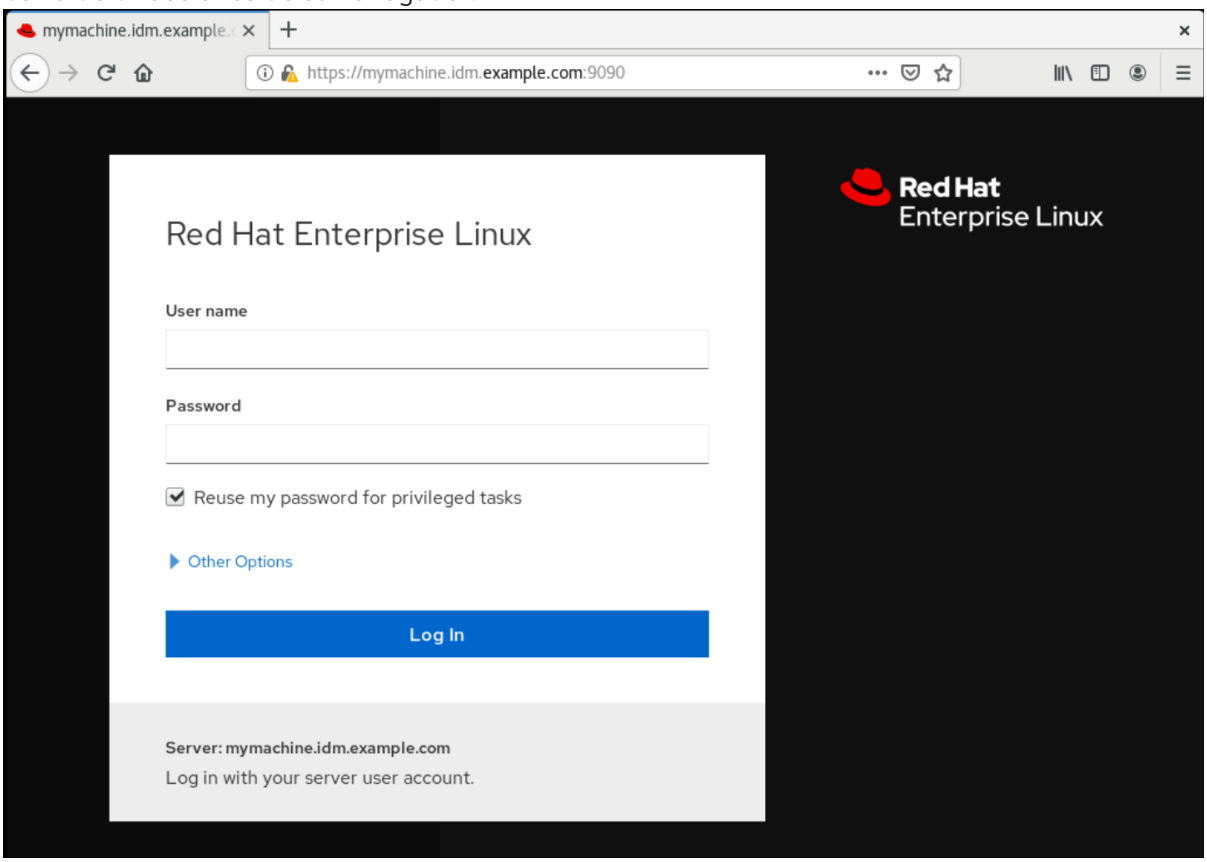
6. Haga clic en **Cambiar**.



Pasos de verificación

1. Cierre la sesión de la consola web.

2. Vuelva a abrir la consola web introduciendo una dirección con el nuevo nombre de host en la barra de direcciones de su navegador.



1.3. COMPLEMENTOS DE LA CONSOLA WEB DE RED HAT

Instale los complementos en la consola web de RHEL 8 y conozca las aplicaciones complementarias disponibles para usted.

1.3.1. Instalación de complementos

El paquete **cockpit** forma parte de Red Hat Enterprise Linux 8 por defecto. Para poder utilizar aplicaciones complementarias debe instalarlas por separado.

Requisitos previos

- Instalado y habilitado el paquete **cockpit**. Si necesita instalar primero la consola web, consulte la sección de instalación.

Procedimiento

- Instala un complemento.

```
# yum install <add-on>
```

1.3.2. Complementos para la consola web de RHEL 8

La siguiente tabla enumera las aplicaciones complementarias disponibles para la consola web de RHEL 8.

Nombre de la característica	Nombre del paquete	Uso
Compositor	cockpit-composer	Creación de imágenes de SO personalizadas
Tablero de mandos	cabina de mando-tablero	Gestión de varios servidores en una sola interfaz de usuario
Máquinas	cabina-máquinas	Gestión de máquinas virtuales libvirt
PackageKit	cockpit-packagekit	Actualizaciones de software e instalación de aplicaciones (normalmente se instalan por defecto)
PCP	cabina-pcp	Datos de rendimiento persistentes y más detallados (instalados a petición de la interfaz de usuario)
podman	cabina-podman	Gestión de contenedores podman (disponible desde RHEL 8.1)
Grabación de la sesión	sesión de cabina-grabación	Grabación y gestión de las sesiones de los usuarios

1.4. OPTIMIZACIÓN DEL RENDIMIENTO DEL SISTEMA MEDIANTE LA CONSOLA WEB

Aprenda a establecer un perfil de rendimiento en la consola web de RHEL 8 para optimizar el rendimiento del sistema para una tarea seleccionada.

1.4.1. Opciones de ajuste del rendimiento en la consola web

Red Hat Enterprise Linux 8 proporciona varios perfiles de rendimiento que optimizan el sistema para las siguientes tareas:

- Sistemas que utilizan el escritorio
- Rendimiento de la producción
- Rendimiento de la latencia
- Rendimiento de la red
- Bajo consumo de energía
- Máquinas virtuales

El servicio **tuned** optimiza las opciones del sistema para ajustarse al perfil seleccionado.

En la consola web, puedes establecer qué perfil de rendimiento utiliza tu sistema.

Recursos adicionales

- Para más detalles sobre el servicio **tuned**, véase Supervisión y gestión del estado y el rendimiento del sistema.

1.4.2. Establecer un perfil de rendimiento en la consola web

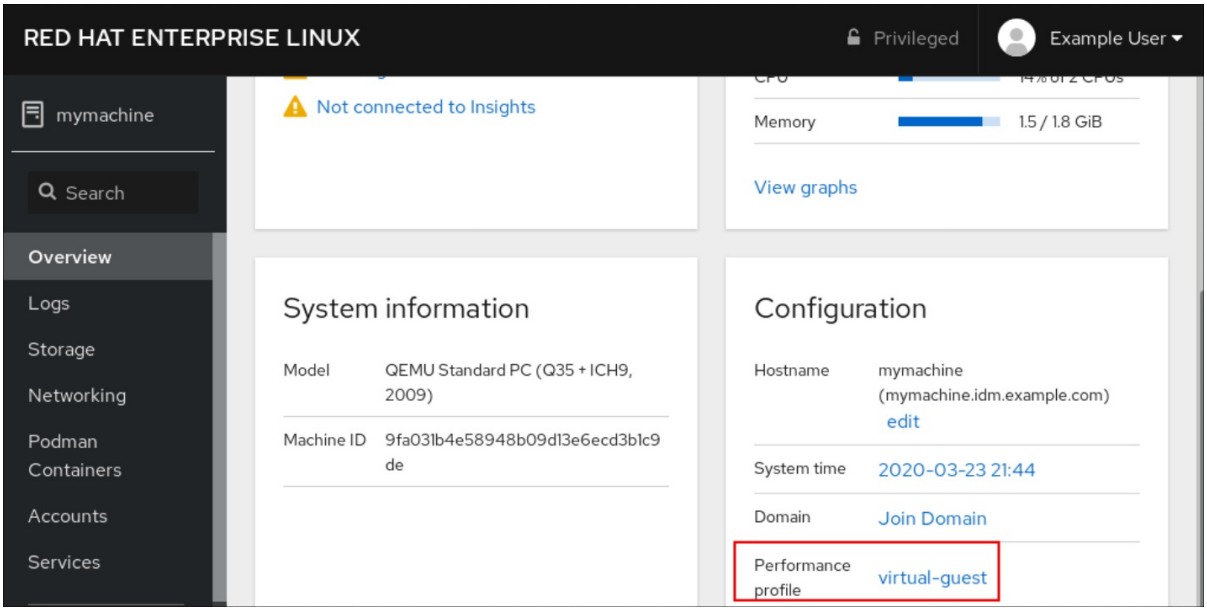
Este procedimiento utiliza la consola web para optimizar el rendimiento del sistema para una tarea seleccionada.

Requisitos previos

- La consola web está instalada y accesible.
  Para más detalles, véase Instalación de la consola web .

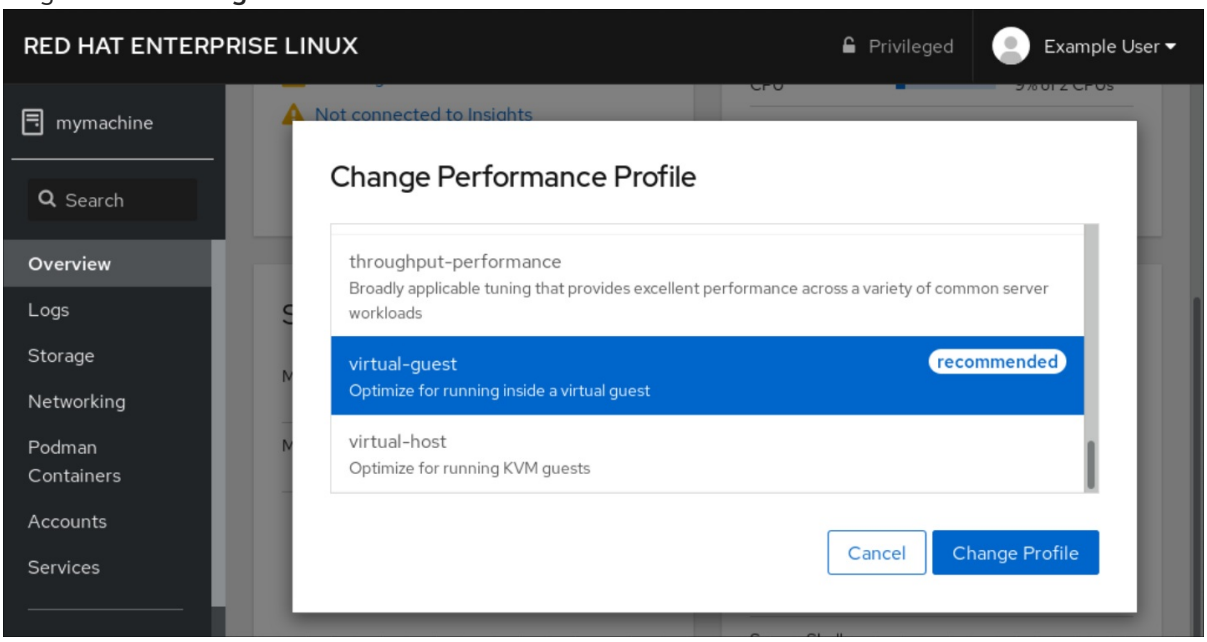
Procedimiento

1. Inicie sesión en la consola web de RHEL 8.
   Para más detalles, consulte Iniciar sesión en la consola web .
2. Haga clic en **Overview**.
3. En el campo **Performance Profile**, haga clic en el perfil de rendimiento actual.



4. En el cuadro de diálogo **Change Performance Profile**, cambie el perfil si es necesario.

5. Haga clic en **Change Profile**.



Pasos de verificación

- La pestaña **Overview** muestra ahora el perfil de rendimiento seleccionado.

1.5. INTRODUCCIÓN A LOS ROLES DE SISTEMA DE RHEL

En esta sección se explica qué son los roles de sistema de RHEL. Además, se describe cómo aplicar un rol particular a través de un playbook de Ansible para realizar varias tareas de administración del sistema.

1.5.1. Introducción a los roles del sistema RHEL

RHEL System Roles es una colección de roles y módulos de Ansible. RHEL System Roles proporciona una interfaz de configuración para gestionar de forma remota varios sistemas RHEL. La interfaz permite gestionar las configuraciones del sistema en varias versiones de RHEL, así como adoptar nuevas versiones principales.

En Red Hat Enterprise Linux 8, la interfaz consta actualmente de los siguientes roles:

- kdump
- red
- selinux
- almacenamiento
- certificado
- kernel_settings
- registro
- métrica
- nbde_client y nbde_server
- timesync
- tlog

Todos estos roles son proporcionados por el paquete **rhel-system-roles** disponible en el repositorio **AppStream**.

Recursos adicionales

- Para obtener una visión general de las funciones del sistema RHEL, consulte el artículo de la base de conocimientos de Red Hat Enterprise Linux (RHEL) sobre las funciones del sistema .
- Para obtener información sobre una función concreta, consulte la documentación en el directorio **/usr/share/doc/rhel-system-roles**. Esta documentación se instala automáticamente con el paquete **rhel-system-roles**.
- Introducción al rol del sistema SELinux
- Introducción a la función de almacenamiento

1.5.2. Terminología de los roles del sistema RHEL

Puede encontrar los siguientes términos en esta documentación:

Terminología de los roles del sistema

Libro de jugadas de Ansible

Los playbooks son el lenguaje de configuración, despliegue y orquestación de Ansible. Pueden describir una política que desea que sus sistemas remotos apliquen, o un conjunto de pasos en un proceso general de TI.

Nodo de control

Cualquier máquina con Ansible instalado. Puedes ejecutar comandos y playbooks, invocando /usr/bin/ansible o /usr/bin/ansible-playbook, desde cualquier nodo de control. Puedes usar cualquier ordenador que tenga Python instalado como nodo de control: ordenadores portátiles,

escritorios compartidos y servidores pueden ejecutar Ansible. Sin embargo, no puedes usar una máquina Windows como nodo de control. Puedes tener varios nodos de control.

Inventario

Una lista de nodos gestionados. Un archivo de inventario también se llama a veces "archivo de host". Su inventario puede especificar información como la dirección IP para cada nodo gestionado. Un inventario también puede organizar los nodos gestionados, creando y anidando grupos para facilitar el escalado. Para obtener más información sobre el inventario, consulte la sección Trabajar con el inventario.

Nodos gestionados

Los dispositivos de red, servidores, o ambos, que gestionas con Ansible. Los nodos gestionados también se denominan a veces "hosts". Ansible no se instala en los nodos gestionados.

1.5.3. Aplicar un papel

El siguiente procedimiento describe cómo aplicar un rol particular.

Requisitos previos

- El paquete **rhel-system-roles** está instalado en el sistema que se quiere utilizar como nodo de control:

```
# yum install rhel-system-roles
```

- El repositorio del motor Ansible está habilitado y el paquete **ansible** está instalado en el sistema que desea utilizar como nodo de control. Necesita el paquete **ansible** para ejecutar playbooks que utilicen RHEL System Roles.
  - Si no dispone de una suscripción a Red Hat Ansible Engine, puede utilizar una versión soportada limitada de Red Hat Ansible Engine proporcionada con su suscripción a Red Hat Enterprise Linux. En este caso, siga estos pasos:
    1. Habilite el repositorio del motor Ansible de RHEL:

```
# subscription-manager refresh
# subscription-manager repos --enable ansible-2-for-rhel-8-x86_64-rpms
```

    2. Instale el motor Ansible:

```
# yum install ansible
```

  - Si tiene una suscripción a Red Hat Ansible Engine, siga el procedimiento descrito en ¿Cómo descargo e instalo Red Hat Ansible Engine?

- Puedes crear un playbook de Ansible.
  Los playbooks representan el lenguaje de configuración, despliegue y orquestación de Ansible. Mediante el uso de playbooks, puedes declarar y gestionar configuraciones de máquinas remotas, desplegar múltiples máquinas remotas u orquestar pasos de cualquier proceso manual ordenado.

  Un playbook es una lista de uno o más **plays**. Cada **play** puede incluir variables, tareas o roles de Ansible.

  Los libros de jugadas son legibles para las personas y se expresan en el formato **YAML**.

Para más información sobre los playbooks, consulte la documentación de Ansible .

Procedimiento

1. Cree un playbook de Ansible que incluya el rol requerido.
   El siguiente ejemplo muestra cómo utilizar los roles a través de la opción **roles:** para un determinado **play**:

```
---
- hosts: webservers
  roles:
    - rhel-system-roles.network
    - rhel-system-roles.timesync
```

   Para más información sobre el uso de roles en los playbooks, consulte la documentación de Ansible.

   Consulte los ejemplos de Ansible para ver ejemplos de playbooks.

NOTA

Cada rol incluye un archivo README, que documenta cómo usar el rol y los valores de los parámetros soportados. También puede encontrar un ejemplo de libro de jugadas para un rol en particular en el directorio de documentación del rol. Este directorio de documentación se proporciona por defecto con el paquete **rhel-system-roles**, y se puede encontrar en la siguiente ubicación:

```
/usr/share/doc/rhel-system-roles/SUBSYSTEM/
```

Sustituya *SUBSYSTEM* por el nombre del rol requerido, como **selinux**, **kdump**, **network**, **timesync**, o **storage**.

2. Verifique la sintaxis del libro de jugadas:

```
# ansible-playbook --syntax-check name.of.the.playbook
```

   El comando **ansible-playbook** ofrece una opción **--syntax-check** que puede utilizar para verificar la sintaxis de un libro de jugadas.

3. Ejecute el libro de jugadas en los hosts seleccionados ejecutando el comando **ansible-playbook**:

```
# ansible-playbook -i name.of.the.inventory name.of.the.playbook
```

   Un inventario es una lista de sistemas con los que trabaja Ansible. Para más información sobre cómo crear un inventario y cómo trabajar con él, consulte la documentación de Ansible .

   Si no tiene un inventario, puede crearlo en el momento de ejecutar **ansible-playbook**:

   Si sólo tiene un host de destino contra el que desea ejecutar el libro de jugadas, utilice:

```
# ansible-playbook -i host1, name.of.the.playbook
```

Si tiene varios hosts de destino contra los que desea ejecutar el libro de jugadas, utilice:

```
# ansible-playbook -i host1,host2,....,hostn name.of.the.playbook
```

Recursos adicionales

- Para obtener información más detallada sobre el uso del comando **ansible-playbook**, consulte la página de manual **ansible-playbook**.

1.5.4. Recursos adicionales

- Para obtener una visión general de las funciones del sistema RHEL, consulte el artículo de la base de conocimientos de Red Hat Enterprise Linux (RHEL) sobre las funciones del sistema .
- Gestión del almacenamiento local mediante los roles de sistema de RHEL
- Despliegue de la misma configuración de SELinux en múltiples sistemas usando RHEL System Roles

1.6. CAMBIO DE LA CONFIGURACIÓN BÁSICA DEL ENTORNO

La configuración de los ajustes básicos del entorno forma parte del proceso de instalación. Las siguientes secciones le guiarán cuando las modifique posteriormente. La configuración básica del entorno incluye:

- Fecha y hora
- Localidades del sistema
- Disposición del teclado
- Idioma

1.6.1. Configurar la fecha y la hora

La precisión en la medición del tiempo es importante por varias razones. En Red Hat Enterprise Linux, el mantenimiento de la hora está garantizado por el protocolo **NTP**, que está implementado por un demonio que se ejecuta en el espacio de usuario. El demonio del espacio de usuario actualiza el reloj del sistema que se ejecuta en el kernel. El reloj del sistema puede mantener la hora utilizando varias fuentes de reloj.

Red Hat Enterprise Linux 8 utiliza el demonio **chronyd** para implementar **NTP**. **chronyd** está disponible en el paquete **chrony** paquete. Para más información, consulte Uso de la suite chrony para configurar NTP.

1.6.1.1. Visualización de la fecha y la hora actuales

Para mostrar la fecha y la hora actuales, utilice cualquiera de estos pasos.

Procedimiento

1. Introduzca el comando **date**:

```
$ date
Mon Mar 30 16:02:59 CEST 2020
```

2. Para ver más detalles, utilice el comando **timedatectl**:

```
$ timedatectl
Local time: Mon 2020-03-30 16:04:42 CEST
Universal time: Mon 2020-03-30 14:04:42 UTC
  RTC time: Mon 2020-03-30 14:04:41
 Time zone: Europe/Prague (CEST, +0200)
System clock synchronized: yes
NTP service: active
RTC in local TZ: no
```

Recursos adicionales

- Para más información, consulte las páginas de manual **date(1)** y **timedatectl(1)**.

1.6.1.2. Recursos adicionales

- Para más información sobre la configuración de la hora en la consola web, consulte Uso de la consola web para configurar la hora.

1.6.2. Configuración de la configuración regional del sistema

La configuración regional de todo el sistema se almacena en el archivo **/etc/locale.conf**, que el demonio **systemd** lee al inicio del sistema. Cada servicio o usuario hereda la configuración regional configurada en **/etc/locale.conf**, a menos que los programas individuales o los usuarios individuales la anulen.

Esta sección describe cómo gestionar la configuración regional del sistema.

Procedimiento

1. Para listar la configuración regional del sistema disponible:

```
$ localectl list-locales
C.utf8
aa_DJ
aa_DJ.iso88591
aa_DJ.utf8
...
```

2. Para mostrar el estado actual de la configuración de locales del sistema:

```
$ localectl status
```

3. Para establecer o cambiar la configuración regional predeterminada del sistema, utilice un subcomando de **localectl set-locale** como usuario de **root**. Por ejemplo:

```
# localectl set-locale LANG=en-US
```

Recursos adicionales

- Para más información, consulte las páginas de manual **localectl(1)**, **locale(7)**, y **locale.conf(5)**.

1.6.3. Configurar la disposición del teclado

La configuración de la disposición del teclado controla la disposición utilizada en la consola de texto y en las interfaces gráficas de usuario.

Procedimiento

1. Para listar los mapas de teclas disponibles:

```
$ localectl list-keymaps
ANSI-dvorak
al
al-plisi
amiga-de
amiga-us
...
```

2. Para mostrar el estado actual de la configuración de los mapas de teclas:

```
$ localectl status
...
VC Keymap: us
...
```

3. Para establecer o cambiar el mapa de teclas por defecto del sistema, utilice un subcomando **localectl set-keymap** como usuario de **root**. Por ejemplo:

```
# localectl set-keymap us
```

Recursos adicionales

- Para más información, consulte las páginas de manual **localectl(1)**, **locale(7)**, y **locale.conf(5)**.

1.6.4. Cambio de idioma mediante la GUI del escritorio

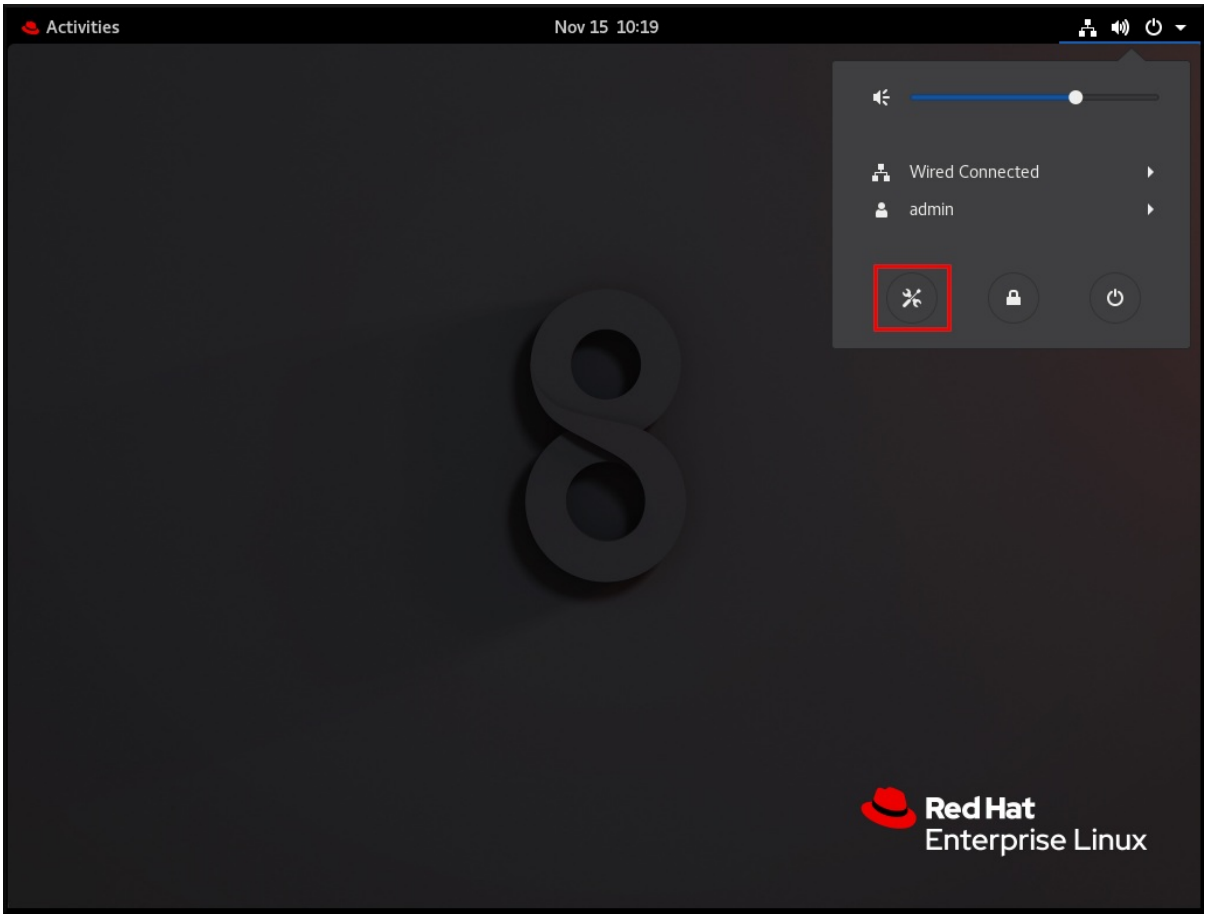
Esta sección describe cómo cambiar el idioma del sistema utilizando la GUI del escritorio.

Requisitos previos

- Los paquetes de idiomas necesarios están instalados en su sistema

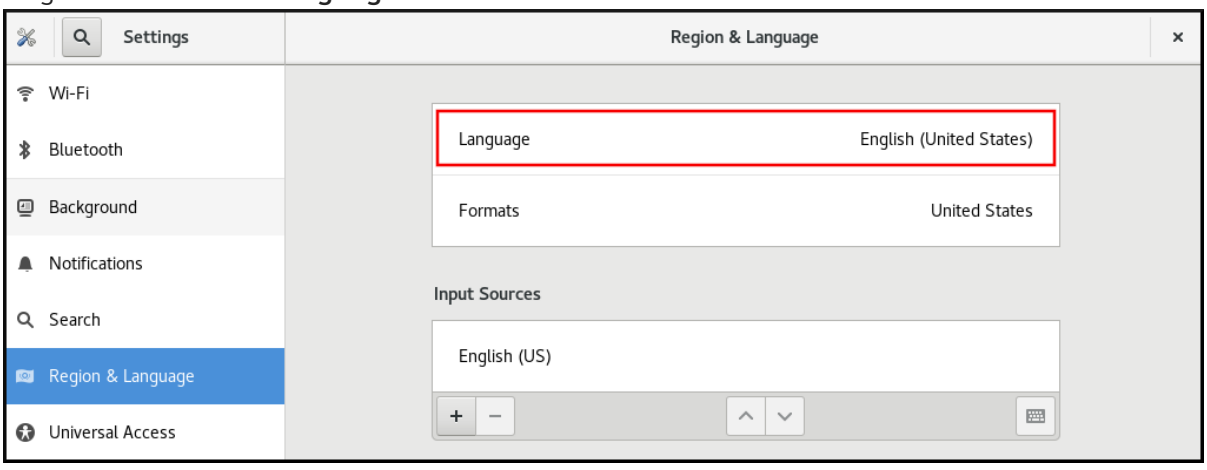
Procedimiento

1. Abra el **GNOME Control Center** desde el **System menu** haciendo clic en su icono.



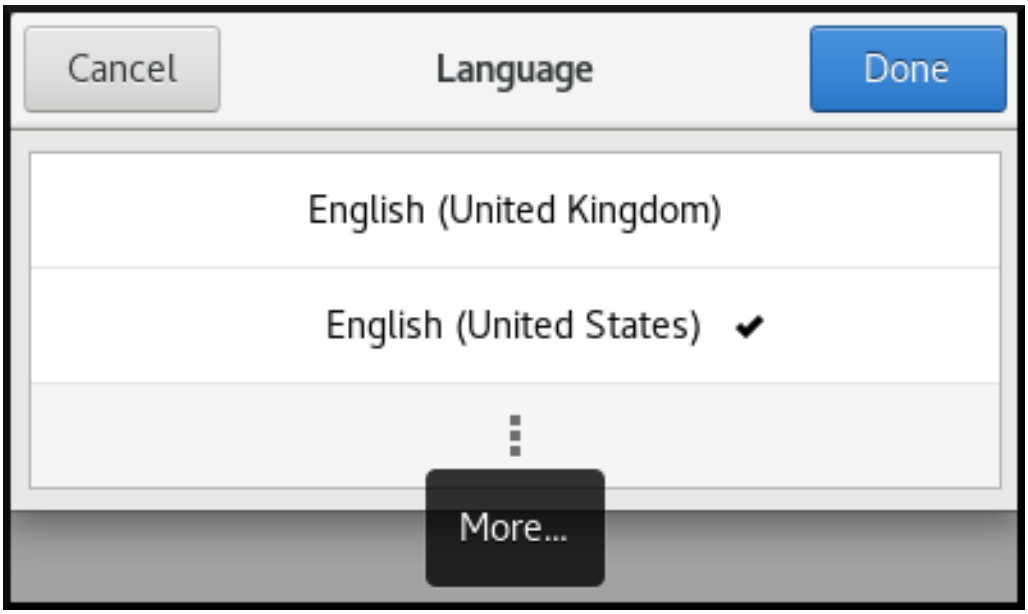
2. En la página **GNOME Control Center**, seleccione **Region & Language** en la barra vertical de la izquierda.

3. Haga clic en el menú **Language**.



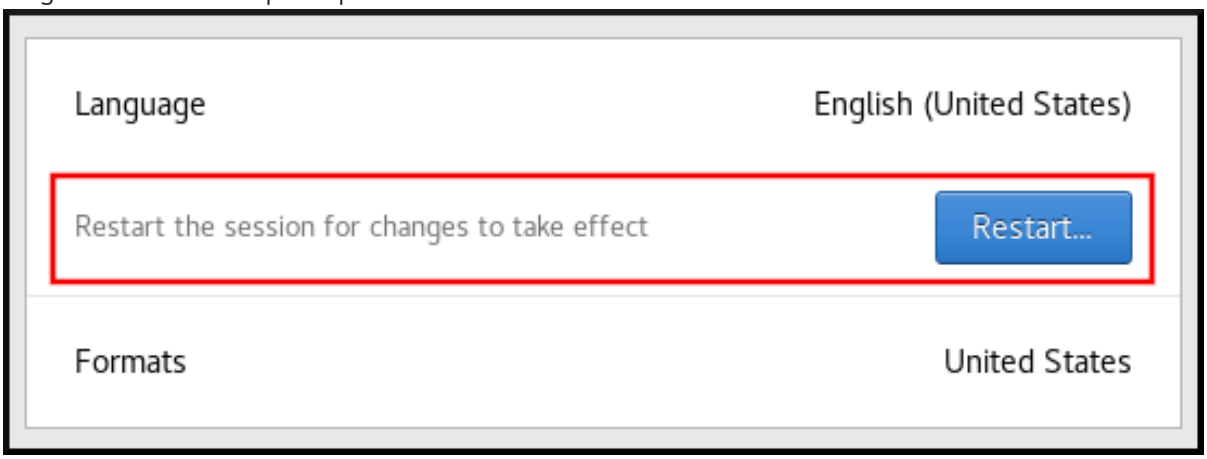
4. Seleccione la región y el idioma deseado en el menú.

Si su región e idioma no aparecen en la lista, desplácese hacia abajo y haga clic en **More** para seleccionar las regiones e idiomas disponibles.



5. Haga clic en **Done**.

6. Haga clic en **Restart** para que los cambios surtan efecto.



NOTA

Algunas aplicaciones no admiten ciertos idiomas. El texto de una aplicación que no puede traducirse al idioma seleccionado permanece en inglés estadounidense.

Recursos adicionales

- Para más información sobre cómo lanzar el **GNOME Control Center**, consulte los enfoques descritos en Lanzamiento de aplicaciones

1.6.5. Recursos adicionales

- Para obtener más información sobre la configuración de los parámetros básicos del entorno, consulte Cómo realizar una instalación estándar de RHEL .

1.7. CONFIGURAR Y GESTIONAR EL ACCESO A LA RED

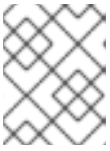
Esta sección describe diferentes opciones sobre cómo añadir conexiones Ethernet en Red Hat Enterprise Linux.

1.7.1. Configurar la red y el nombre de host en el modo de instalación gráfica

Siga los pasos de este procedimiento para configurar su red y su nombre de host.

Procedimiento

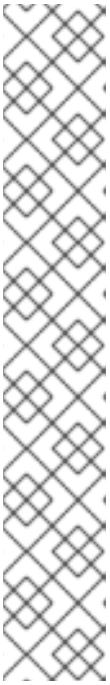
1. En la ventana **Installation Summary**, haga clic en **Red y Nombre de host***.
2. En la lista del panel izquierdo, seleccione una interfaz. Los detalles se muestran en el panel derecho.
3. Activa el interruptor **ON**/**OFF** para activar o desactivar la interfaz seleccionada.



NOTA

El programa de instalación detecta automáticamente las interfaces accesibles localmente, y no se pueden añadir o eliminar manualmente.

4. Haga clic en para añadir una interfaz de red virtual, que puede ser: Equipo, Enlace, Puente o VLAN.
5. Haga clic en **-** para eliminar una interfaz virtual.
6. Haga clic en **Configurar** para cambiar los ajustes como las direcciones IP, los servidores DNS o la configuración de enrutamiento para una interfaz existente (tanto virtual como física).
7. Introduzca un nombre de host para su sistema en el campo **Host Name**.



NOTA

- Existen varios tipos de estándares de denominación de dispositivos de red que se utilizan para identificar los dispositivos de red con nombres persistentes, por ejemplo, **em1** y **wl3sp0**. Para obtener información sobre estos estándares, consulte el *Configuring and managing networking* documento.

- El nombre de host puede ser un nombre de dominio completamente calificado (FQDN) en el formato *hostname.domainname*, o un nombre de host corto sin nombre de dominio. Muchas redes tienen un servicio de Protocolo de Configuración Dinámica de Host (DHCP) que proporciona automáticamente a los sistemas conectados un nombre de dominio. Para permitir que el servicio DHCP asigne el nombre de dominio a esta máquina, especifique sólo el nombre de host corto. El valor **localhost.localdomain** significa que no se configura ningún nombre de host estático específico para el sistema de destino, y que el nombre de host real del sistema instalado se configura durante el procesamiento de la configuración de la red, por ejemplo, mediante **NetworkManager** utilizando DHCP o DNS.

8. Haga clic en **Aplicar** para aplicar el nombre del host al entorno.

Recursos e información adicionales

- Para obtener detalles sobre la configuración de los ajustes de red y el nombre del host cuando se utiliza un archivo Kickstart, consulte el apéndice correspondiente en Realización de una instalación avanzada de RHEL.

- Si instala Red Hat Enterprise Linux utilizando el modo de texto del programa de instalación **Anaconda**, utilice la opción **Configuración de red** para configurar la red.

1.7.2. Configuración de una conexión Ethernet estática mediante nmcli

Este procedimiento describe la adición de una conexión Ethernet con la siguiente configuración utilizando la utilidad **nmcli**:

- Una dirección IPv4 estática - **192.0.2.1** con una máscara de subred **/24**
- Una dirección IPv6 estática - **2001:db8:1::1** con una máscara de subred **/64**
- Una pasarela por defecto IPv4 - **192.0.2.254**
- Una pasarela por defecto IPv6 - **2001:db8:1::fffe**
- Un servidor DNS IPv4 - **192.0.2.200**
- Un servidor DNS IPv6 - **2001:db8:1::ffbb**
- Un dominio de búsqueda DNS - **example.com**

Procedimiento

1. Añade un nuevo perfil de conexión NetworkManager para la conexión Ethernet:

```
# nmcli connection add con-name Example-Connection ifname enp7s0 type ethernet
```

Los pasos siguientes modifican el perfil de conexión **Example-Connection** que ha creado.

2. Establezca la dirección IPv4:

```
# nmcli connection modify Example-Connection ipv4.addresses 192.0.2.1/24
```

3. Establezca la dirección IPv6:

```
# nmcli connection modify Example-Connection ipv6.addresses 2001:db8:1::1/64
```

4. Establezca el método de conexión IPv4 e IPv6 en **manual**:

```
# nmcli connection modify Example-Connection ipv4.method manual
# nmcli connection modify Example-Connection ipv6.method manual
```

5. Establezca las pasarelas por defecto IPv4 e IPv6:

```
# nmcli connection modify Example-Connection ipv4.gateway 192.0.2.254
# nmcli connection modify Example-Connection ipv6.gateway 2001:db8:1::fffe
```

6. Establezca las direcciones de los servidores DNS IPv4 e IPv6:

```
# nmcli connection modify Example-Connection ipv4.dns "192.0.2.200"
# nmcli connection modify Example-Connection ipv6.dns "2001:db8:1::ffbb"
```

Para establecer varios servidores DNS, especifíquelos separados por espacios y encerrados entre comillas.

7. Establezca el dominio de búsqueda DNS para la conexión IPv4 e IPv6:

```
# nmcli connection modify Example-Connection ipv4.dns-search example.com
# nmcli connection modify Example-Connection ipv6.dns-search example.com
```

8. Activar el perfil de conexión:

```
# nmcli connection up Example-Connection
Connection successfully activated (D-Bus active path:
/org/freedesktop/NetworkManager/ActiveConnection/13)
```

Pasos de verificación

1. Muestra el estado de los dispositivos y las conexiones:

```
# nmcli device status
DEVICE     TYPE      STATE      CONNECTION
enp7s0     ethernet  connected  Example-Connection
```

2. Para mostrar todos los ajustes del perfil de conexión:

```
# nmcli connection show Example-Connection
connection.id:                Example-Connection
connection.uuid:              b6cdfa1c-e4ad-46e5-af8b-a75f06b79f76
connection.stable-id:         --
```

```
connection.type:          802-3-ethernet
connection.interface-name:  enp7s0
...
```

3. Utilice la utilidad **ping** para verificar que este host puede enviar paquetes a otros hosts.

   - Hacer ping a una dirección IP en la misma subred.
     Para IPv4:

     ```
     # ping 192.0.2.3
     ```

     Para IPv6:

     ```
     # ping 2001:db8:2::1
     ```

     Si el comando falla, verifique la configuración de la IP y la subred.

   - Hacer ping a una dirección IP en una subred remota.
     Para IPv4:

     ```
     # ping 198.162.3.1
     ```

     Para IPv6:

     ```
     # ping 2001:db8:2::1
     ```

     - Si el comando falla, haga un ping a la puerta de enlace por defecto para verificar la configuración.
       Para IPv4:

       ```
       # ping 192.0.2.254
       ```

       Para IPv6:

       ```
       # ping 2001:db8:1::fffe
       ```

4. Utilice la utilidad **host** para verificar que la resolución de nombres funciona. Por ejemplo:

   ```
   # host client.example.com
   ```

   Si el comando devuelve algún error, como **connection timed out** o **no servers could be reached**, verifique su configuración de DNS.

Pasos para la resolución de problemas

1. Si la conexión falla o si la interfaz de red cambia entre un estado de subida y de bajada:

   - Asegúrese de que el cable de red está conectado al host y a un conmutador.
   - Compruebe si el fallo de enlace existe sólo en este host o también en otros hosts conectados al mismo switch al que está conectado el servidor.

- Compruebe que el cable de red y la interfaz de red funcionan como se espera. Realice los pasos de diagnóstico de hardware y sustituya los cables y las tarjetas de interfaz de red defectuosos.

Recursos adicionales

- Consulte la página de manual **nm-settings(5)** para obtener más información sobre las propiedades del perfil de conexión y su configuración.
- Para más detalles sobre la utilidad **nmcli**, consulte la página de manual **nmcli(1)**.
- Si la configuración del disco no coincide con la del dispositivo, al iniciar o reiniciar NetworkManager se crea una conexión en memoria que refleja la configuración del dispositivo. Para más detalles y cómo evitar este problema, consulte NetworkManager duplica una conexión después de reiniciar el servicio NetworkManager.
- Si la conexión no tiene una puerta de enlace predeterminada, consulte Configuración de NetworkManager para evitar el uso de un perfil específico para proporcionar una puerta de enlace predeterminada en la documentación de **Configuring and managing networking**.

1.7.3. Añadir un perfil de conexión mediante nmtui

La aplicación **nmtui** proporciona una interfaz de usuario de texto para NetworkManager. Este procedimiento describe cómo añadir un nuevo perfil de conexión.

Requisitos previos

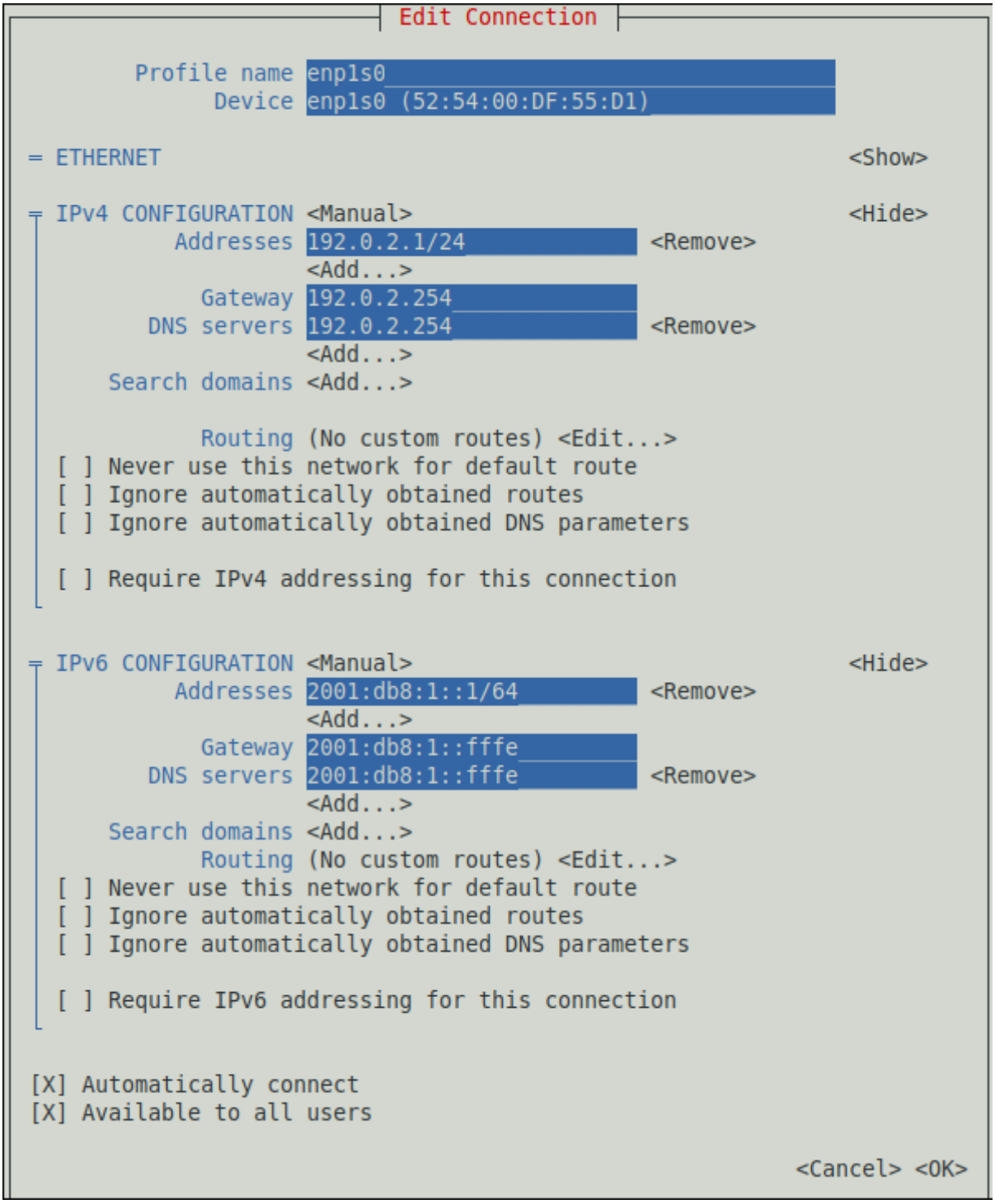
- El paquete **NetworkManager-tui** está instalado.

Procedimiento

1. Inicie la utilidad de interfaz de usuario de texto NetworkManager:

```
# nmtui
```

2. Seleccione la entrada del menú **Edit a connection** y pulse **Intro**.
3. Seleccione el botón **Añadir** y pulse **Intro**.
4. Seleccione **Ethernet** y pulse **Intro**.
5. Rellene los campos con los detalles de la conexión.



6. Seleccione **OK** para guardar los cambios.
7. Seleccione **Back** para volver al menú principal.
8. Seleccione **Activate a connection** y pulse **Intro**.
9. Seleccione la nueva entrada de conexión y pulse **Enter** para activar la conexión.
10. Seleccione **Atrás** para volver al menú principal.
11. Seleccione **Quit**.

Pasos de verificación

1. Muestra el estado de los dispositivos y las conexiones:

```
# nmcli device status
DEVICE      TYPE      STATE      CONNECTION
enp1s0      ethernet  connected  Example-Connection
```

2. Para mostrar todos los ajustes del perfil de conexión:

```
# nmcli connection show Example-Connection
connection.id:                Example-Connection
connection.uuid:              b6cdfa1c-e4ad-46e5-af8b-a75f06b79f76
connection.stable-id:         --
connection.type:              802-3-ethernet
connection.interface-name:    enp1s0
...
```

Recursos adicionales

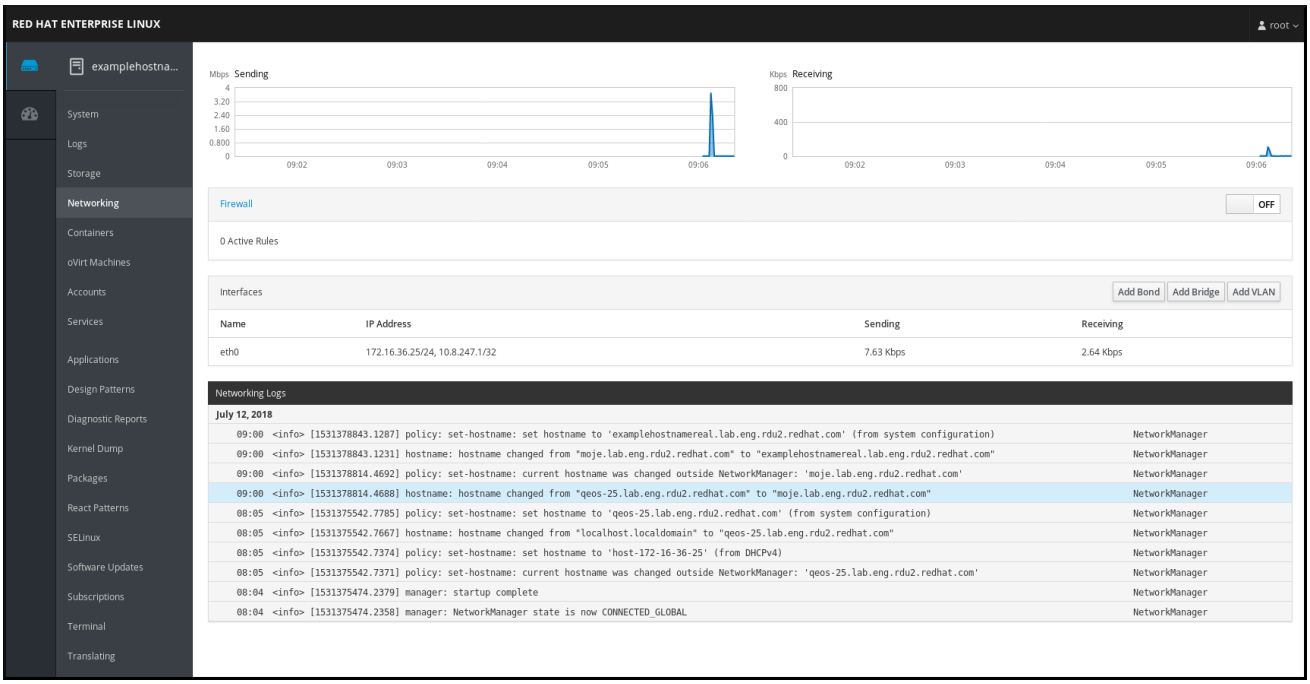
- Para obtener más información sobre la comprobación de las conexiones, consulte Prueba de la configuración básica de la red en **Configuring and managing networking**.
- Para más detalles sobre la aplicación **nmtui**, consulte la página man **nmtui(1)**.
- Si la configuración del disco no coincide con la del dispositivo, al iniciar o reiniciar NetworkManager se crea una conexión en memoria que refleja la configuración del dispositivo. Para más detalles y cómo evitar este problema, consulte NetworkManager duplica una conexión después de reiniciar el servicio NetworkManager.

1.7.4. Gestión de la red en la consola web de RHEL 8

En la consola web, el menú **Red** le permite:

- Para mostrar los paquetes recibidos y enviados actualmente
- Para mostrar las características más importantes de las interfaces de red disponibles
- Para mostrar el contenido de los registros de red.
- Para añadir varios tipos de interfaces de red (enlace, equipo, puente, VLAN)

Figura 1.1. Gestión de la red en la consola web de RHEL 8



1.7.5. Gestión de la red mediante los roles de sistema de RHEL

Puede configurar las conexiones de red en varias máquinas de destino utilizando el rol **network**.

El rol **network** permite configurar los siguientes tipos de interfaces:

- Ethernet
- Puente
- Vinculado
- VLAN
- MacVLAN
- Infiniband

Las conexiones de red necesarias para cada host se proporcionan como una lista dentro de la variable **network_connections**.

AVISO

El rol **network** actualiza o crea todos los perfiles de conexión en el sistema de destino exactamente como se especifica en la variable **network_connections**. Por lo tanto, el rol **network** elimina las opciones de los perfiles especificados si las opciones sólo están presentes en el sistema pero no en la variable **network_connections**.

El siguiente ejemplo muestra cómo aplicar el rol **network** para asegurar que existe una conexión Ethernet con los parámetros requeridos:

Ejemplo 1.3. Un ejemplo de libro de jugadas aplicando el rol de red para configurar una conexión Ethernet con los parámetros requeridos

```
# SPDX-License-Identifier: BSD-3-Clause
---
- hosts: network-test
  vars:
    network_connections:

      # Create one ethernet profile and activate it.
      # The profile uses automatic IP addressing
      # and is tied to the interface by MAC address.
      - name: prod1
        state: up
        type: ethernet
        autoconnect: yes
        mac: "00:00:5e:00:53:00"
        mtu: 1450

  roles:
    - rhel-system-roles.network
```

Para más información sobre la aplicación de un rol de sistema, consulte Introducción a los roles de sistema de RHEL.

1.7.6. Recursos adicionales

- Para obtener más detalles sobre la configuración de la red, como la configuración de la unión de redes y la formación de equipos, consulte el título Configuración y gestión de redes .

1.8. REGISTRO DEL SISTEMA Y GESTIÓN DE LAS SUSCRIPCIONES

Las suscripciones cubren los productos instalados en Red Hat Enterprise Linux, incluido el propio sistema operativo.

Puede utilizar una suscripción a Red Hat Content Delivery Network para realizar un seguimiento:

- Sistemas registrados
- Productos instalados en sus sistemas
- Suscripciones vinculadas a los productos instalados

1.8.1. Registrar el sistema después de la instalación

Utilice el siguiente procedimiento para registrar su sistema si no lo ha registrado ya durante el proceso de instalación.

Requisitos previos

- Una cuenta de usuario válida en el Portal del Cliente de Red Hat.
- Consulte la página Crear un inicio de sesión de Red Hat .
- Una suscripción activa para el sistema RHEL.
- Para obtener más información sobre el proceso de instalación, consulte Cómo realizar una instalación estándar de RHEL.

Procedimiento

1. Registre y suscriba automáticamente su sistema en un solo paso:

```
# subscription-manager register --username <username> --password <password> --auto-attach
Registering to: subscription.rhsm.redhat.com:443/subscription
The system has been registered with ID: 37to907c-ece6-49ea-9174-20b87ajk9ee7
The registered system name is: client1.idm.example.com
Installed Product Current Status:
Product Name: Red Hat Enterprise Linux for x86_64
Status:       Subscribed
```

   El comando le pide que introduzca su nombre de usuario y contraseña del Portal del Cliente de Red Hat.

   Si el proceso de registro falla, puede registrar su sistema con un pool específico. Para obtener orientación sobre cómo hacerlo, siga los siguientes pasos:

   a. Determine el ID de grupo de una suscripción que necesite:

```
# subscription-manager list --available
```

      Este comando muestra todas las suscripciones disponibles para su cuenta de Red Hat. Para cada suscripción, se muestran varias características, incluyendo el ID del pool.

   b. Adjunte la suscripción adecuada a su sistema sustituyendo *pool_id* por el ID de la piscina determinado en el paso anterior:

```
# subscription-manager attach --pool=pool_id
```

Recursos adicionales

- Para obtener más detalles sobre el registro de sistemas RHEL mediante la opción **--auto-attach**, consulte la sección Comprender las suscripciones automáticas en el Portal del Cliente .
- Para obtener más detalles sobre el registro manual de los sistemas RHEL, consulte la sección Comprender el registro manual y la suscripción en el Portal del Cliente .

1.8.2. Registro de suscripciones con credenciales en la consola web

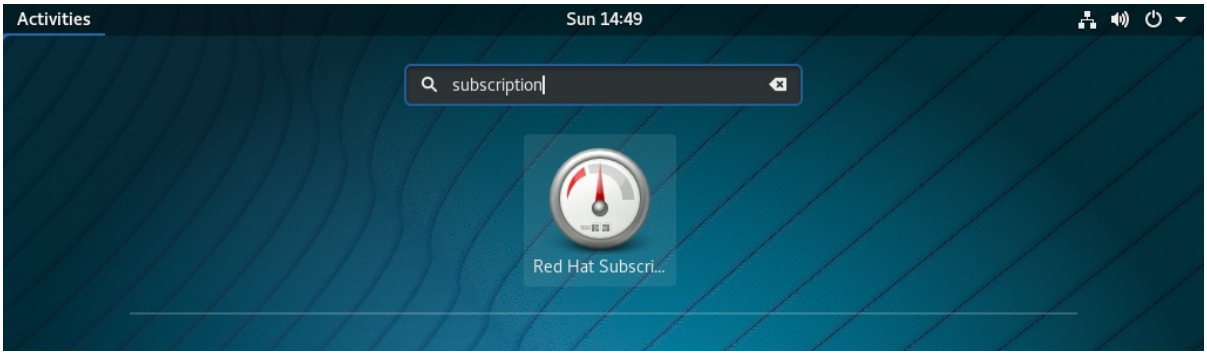
Siga los siguientes pasos para registrar un Red Hat Enterprise Linux recién instalado mediante la consola web de RHEL 8.

Requisitos previos

- Una cuenta de usuario válida en el Portal del Cliente de Red Hat.
  Consulte la página Crear un inicio de sesión de Red Hat .
- Suscripción activa para su sistema RHEL.

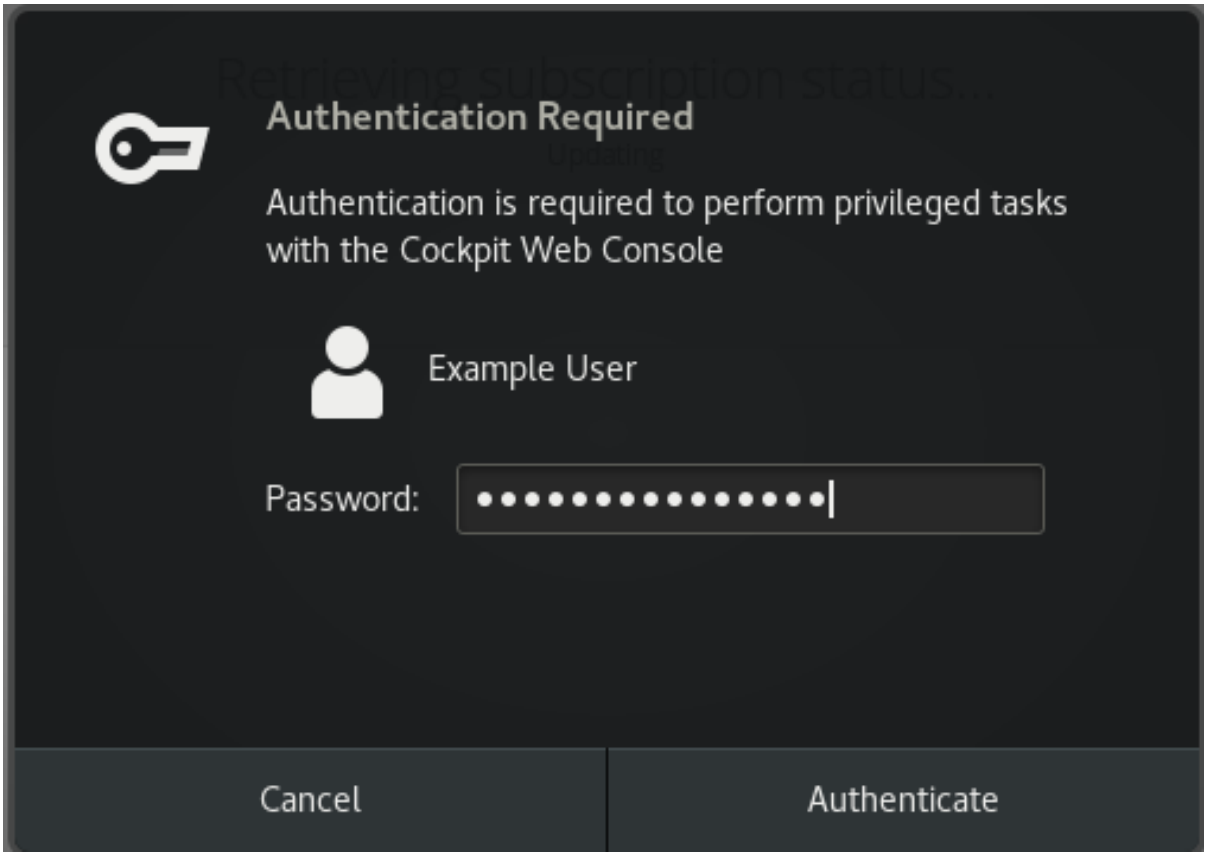
Procedimiento

1. Escriba suscripción en el campo de búsqueda y pulse la tecla **Enter**.

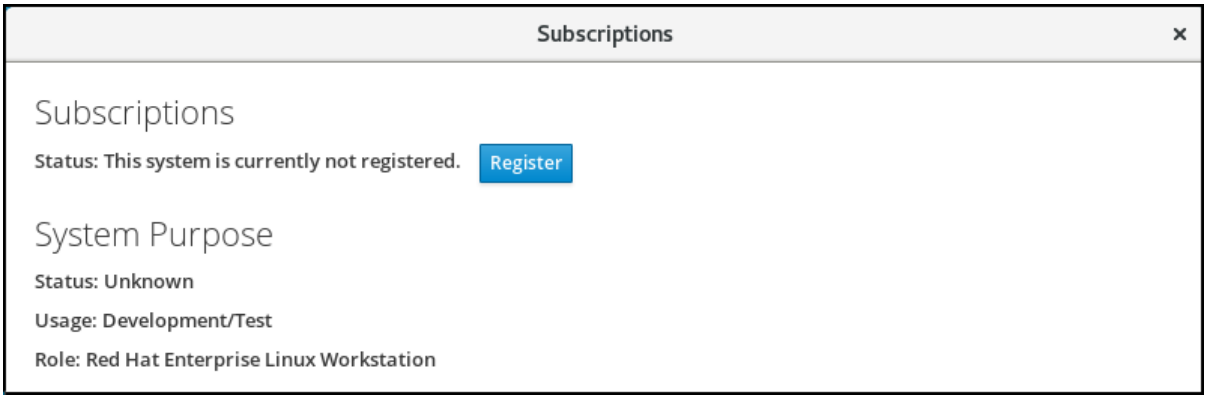


   También puede iniciar sesión en la consola web de RHEL 8. Para más detalles, consulte Iniciar sesión en la consola web.

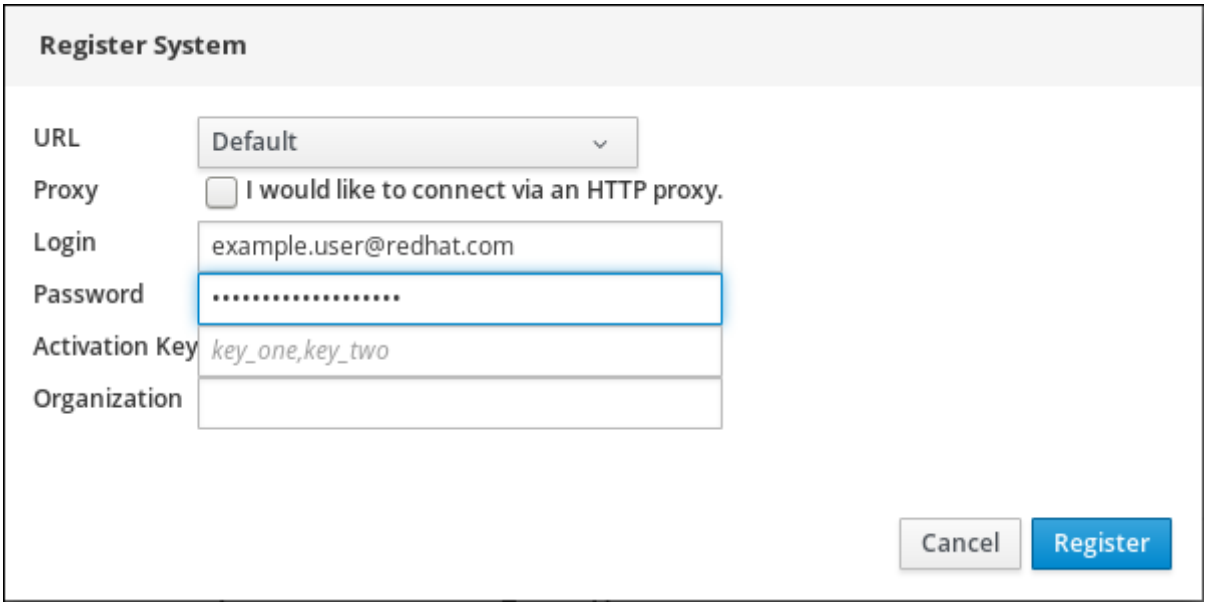
2. En el diálogo de autenticación **polkit** para tareas privilegiadas, añada la contraseña correspondiente al nombre de usuario que aparece en el diálogo.



3. Haga clic en **Autenticar**.
4. En el cuadro de diálogo **Subscriptions**, haga clic en **Registrar**.



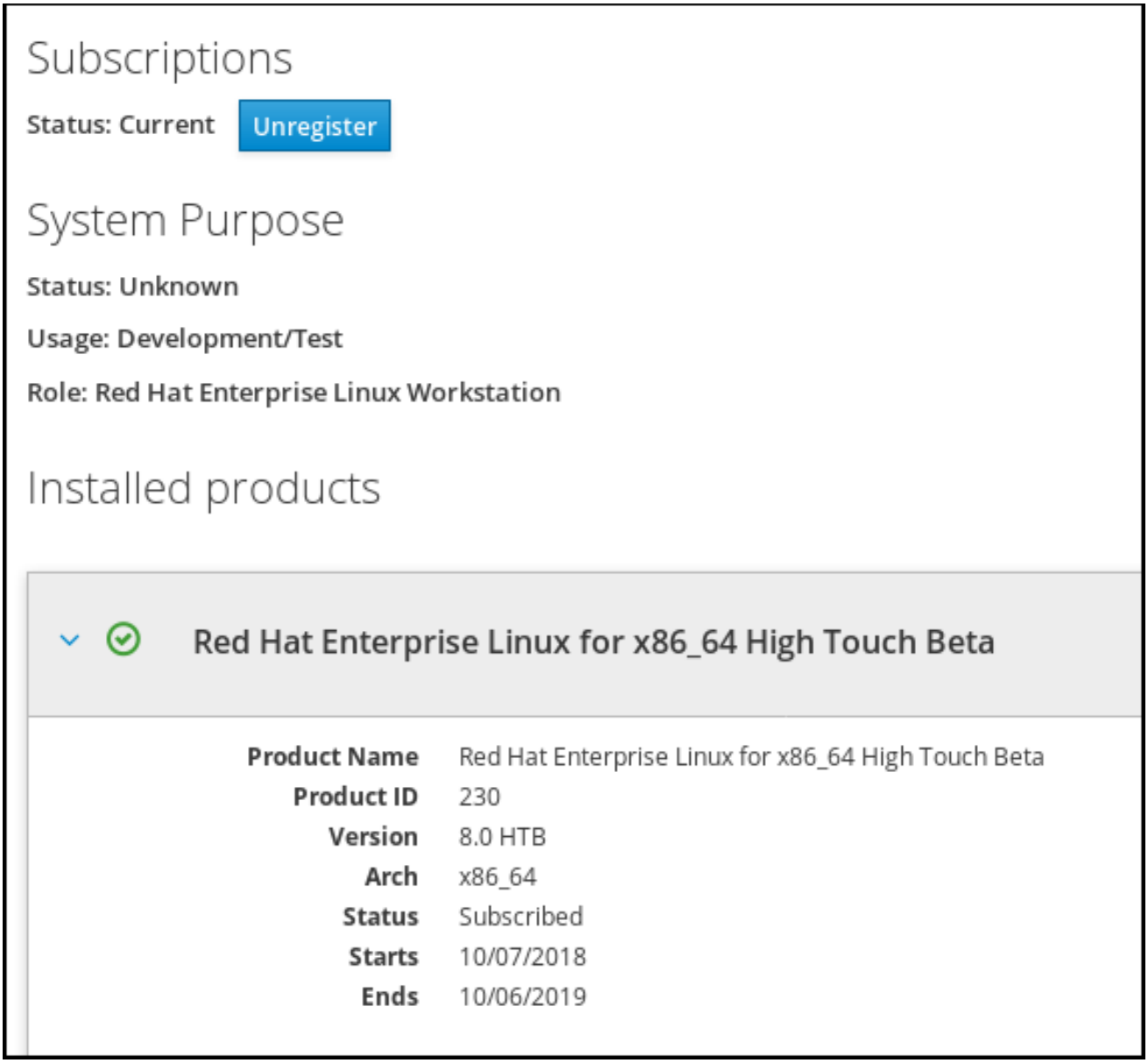
5. Introduzca sus credenciales del Portal del Cliente.



6. Introduzca el nombre de su organización.
   Si tiene más de una cuenta en el Portal del Cliente de Red Hat, tiene que añadir el nombre de la organización o el ID de la organización. Para obtener el ID de la organización, diríjase a su punto de contacto de Red Hat.

7. Haga clic en el botón de **registro**.

En este punto, su sistema Red Hat Enterprise Linux 8 ha sido registrado con éxito.



1.8.3. Registro de un sistema utilizando la cuenta de Red Hat en GNOME

Siga los pasos de este procedimiento para registrar su sistema con su cuenta de Red Hat.

Requisitos previos

- Una cuenta válida en el portal de clientes de Red Hat.
  Consulte la página Crear un inicio de sesión de Red Hat para el registro de nuevos usuarios.

Procedimiento

1. Vaya a la página **system menu**, a la que puede acceder desde la esquina superior derecha de la pantalla, y haga clic en el icono **Settings**.
2. En la sección **Detalles → Acerca de** sección, haga clic en **Registro**.
3. Seleccione **Registration Server**.
4. Si no está utilizando el servidor de Red Hat, introduzca la dirección del servidor en el campo **URL**.

5. En el menú **Registration Type**, seleccione **Red Hat Account**.
6. En **Registration Details**:
   - Introduzca el nombre de usuario de su cuenta Red Hat en el campo **Login**,
   - Introduzca la contraseña de su cuenta Red hat en el campo **Password**.
   - Introduzca el nombre de su organización en el campo **Organization**.
7. Haga clic en **Registrarse**.

1.8.4. Registro de un sistema mediante una clave de activación en GNOME

Siga los pasos de este procedimiento para registrar su sistema con una clave de activación. Puede obtener la clave de activación del administrador de su organización.

Requisitos previos

- Clave o claves de activación.
  Consulte la página de claves de activación para crear nuevas claves de activación.

Procedimiento

1. Vaya a la página **system menu**, a la que puede acceder desde la esquina superior derecha de la pantalla, y haga clic en el icono **Settings**.
2. En la sección **Detalles → Acerca de** sección, haga clic en **Registro**.
3. Seleccione **Registration Server**.
4. Introduzca **URL** en el servidor personalizado, si no está utilizando el servidor de Red Hat.
5. En el menú **Registration Type**, seleccione **Activation Keys**.
6. En **Registration Details**:
   - Entre en **Activation Keys**.
     Separe varias claves con una coma (,).
   - Introduzca el nombre o la identificación de su organización en el campo **Organization**.
7. Haga clic en **Registro**

1.9. HACER QUE LOS SERVICIOS DE SYSTEMD SE INICIEN EN EL ARRANQUE

Systemd es un gestor de sistemas y servicios para sistemas operativos Linux que introduce el concepto de unidades systemd.

Esta sección proporciona información sobre cómo asegurarse de que un servicio está activado o desactivado en el momento del arranque. También explica cómo gestionar los servicios a través de la consola web.

1.9.1. Activar o desactivar los servicios mediante la CLI

Puede determinar qué servicios se activan o desactivan en el momento del arranque ya durante el proceso de instalación. También puede activar o desactivar un servicio en un sistema operativo instalado.

Esta sección describe los pasos para activar o desactivar esos servicios en un sistema operativo ya instalado:

Requisitos previos

- Debe tener acceso a la raíz del sistema.

Procedimiento

1. Para activar un servicio, utilice la opción **enable**:

   ```
   # systemctl enable service_name
   ```

   Sustituya *service_name* por el servicio que desea activar.

   También puede habilitar e iniciar un servicio en un solo comando:

   ```
   # systemctl enable --now service_name
   ```

2. Para desactivar un servicio, utilice la opción **disable**:

   ```
   # systemctl disable service_name
   ```

   Sustituya *service_name* por el servicio que desea desactivar.

AVISO

No se puede habilitar un servicio que haya sido previamente enmascarado. Primero hay que desenmascararlo:

```
# systemctl unmask service_name
```

1.9.2. Gestión de servicios en la consola web de RHEL 8

Esta sección describe cómo puede también habilitar o deshabilitar un servicio usando la consola web. Puedes gestionar los objetivos systemd, los servicios, los sockets, los temporizadores y las rutas. También puede comprobar el estado del servicio, iniciar o detener servicios, habilitarlos o deshabilitarlos.

Requisitos previos

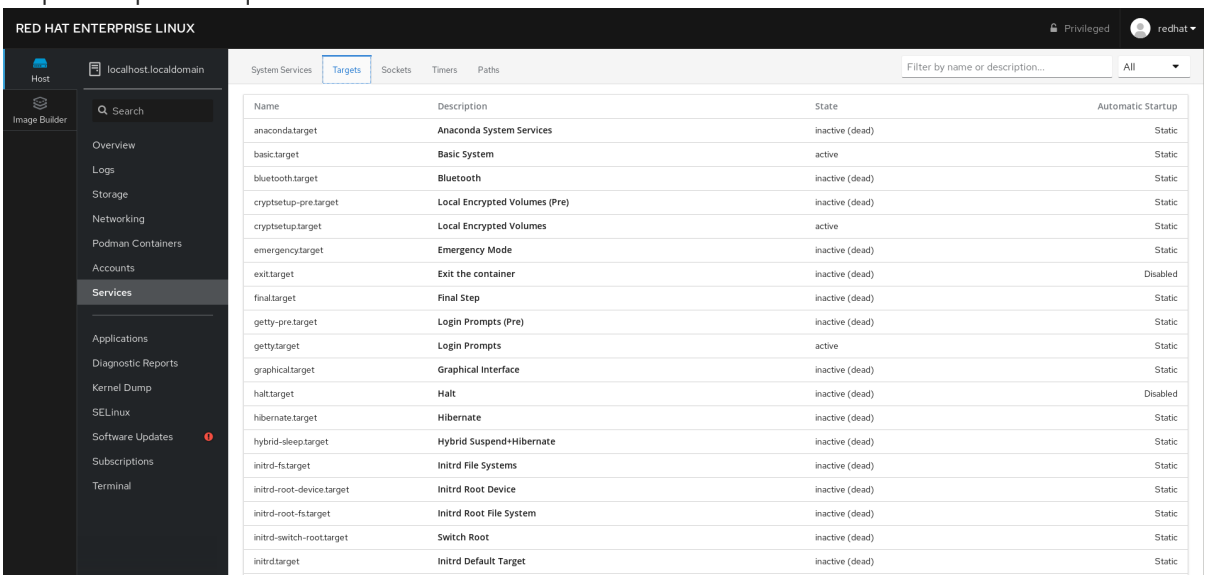
- Debe tener acceso a la raíz del sistema.

Procedimiento

1. Abra **https://localhost:9090/** en un navegador web de su preferencia.

2. Acceda a la consola web con sus credenciales de root en el sistema.

3. Para mostrar el panel de la consola web, haga clic en el icono **Host**, que se encuentra en la esquina superior izquierda de la ventana.



4. En el menú, haga clic en **Servicios**.
Puedes gestionar los objetivos de systemd, los servicios, los sockets, los temporizadores y las rutas.

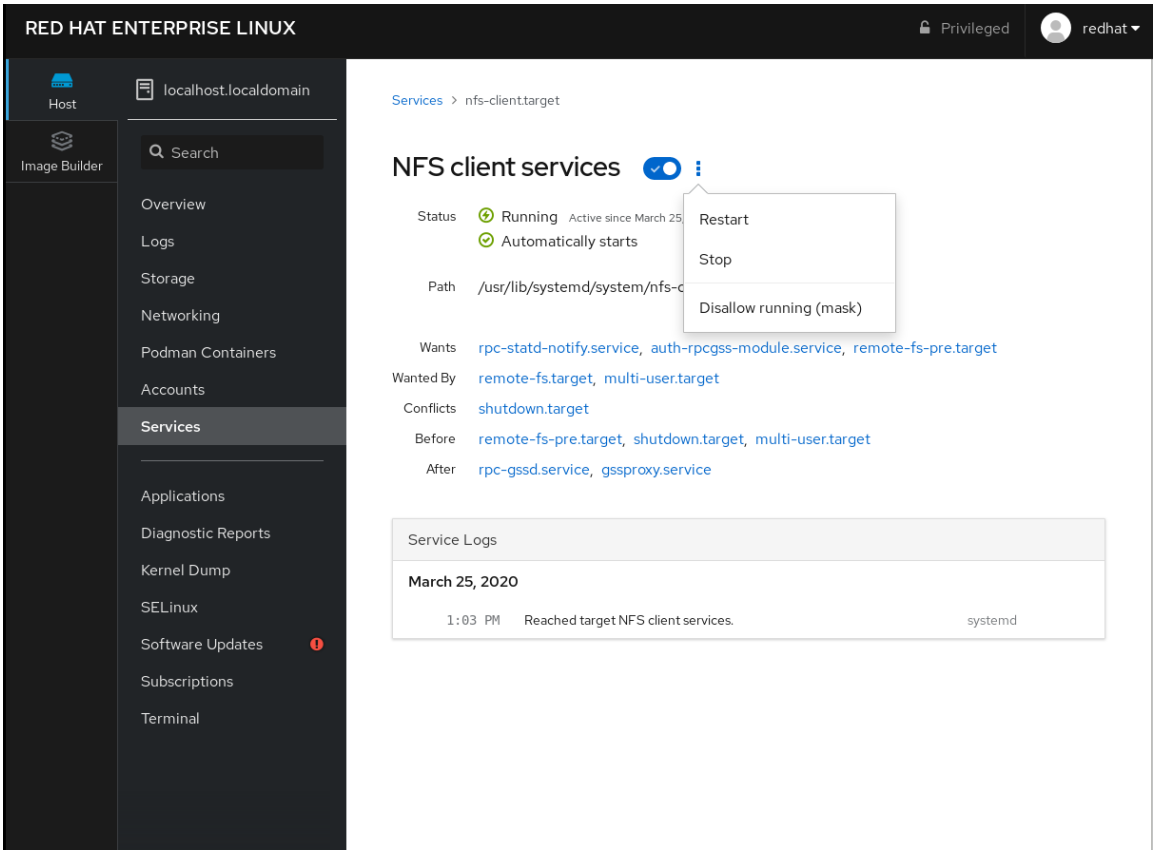
5. Por ejemplo, para gestionar el servicio **NFS client services**:

   a. Haga clic en **los objetivos**.

   b. Seleccione el servicio **NFS client services**.

   c. Para activar o desactivar el servicio, haga clic en el botón **Toogle**.

   d. Para detener el servicio, haga clic en el botón y elija la opción 'Detener'.



1.10. CONFIGURAR LA SEGURIDAD DEL SISTEMA

La seguridad informática es la protección de los sistemas informáticos y su hardware, software, información y servicios frente a robos, daños, interrupciones y desvíos. Garantizar la seguridad informática es una tarea esencial, en particular en las empresas que procesan datos sensibles y manejan transacciones comerciales.

Esta sección cubre solamente las características básicas de seguridad que puede configurar después de la instalación del sistema operativo. Para obtener información detallada sobre la seguridad de Red Hat Enterprise Linux, consulte la sección **Security** en la Documentación del producto para Red Hat Enterprise Linux 8.

1.10.1. Mejorar la seguridad del sistema con un cortafuegos

Un cortafuegos es un sistema de seguridad de red que supervisa y controla el tráfico de red entrante y saliente según las reglas de seguridad configuradas. Un cortafuegos suele establecer una barrera entre una red interna segura de confianza y otra red externa.

El servicio **firewalld**, que proporciona un cortafuegos en Red Hat Enterprise Linux, se activa automáticamente durante la instalación.

1.10.1.1. Habilitación del servicio firewalld

Para activar el servicio **firewalld**, siga este procedimiento.

Procedimiento

1. Muestra el estado actual de **firewalld**:

```
$ systemctl status firewalld
```

```
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor preset:
enabled)
   Active: inactive (dead)
...
```

2. Si **firewalld** no está habilitado y en ejecución, cambie al usuario **root**, e inicie el servicio **firewalld** y habilite para que se inicie automáticamente después de reiniciar el sistema:

```
# systemctl enable --now firewalld
```

Pasos de verificación

1. Compruebe que **firewalld** se está ejecutando y está habilitado:

```
$ systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset:
enabled)
   Active: active (running)
...
```

Recursos adicionales

- Para más información, consulte la página de manual **firewalld(1)**.

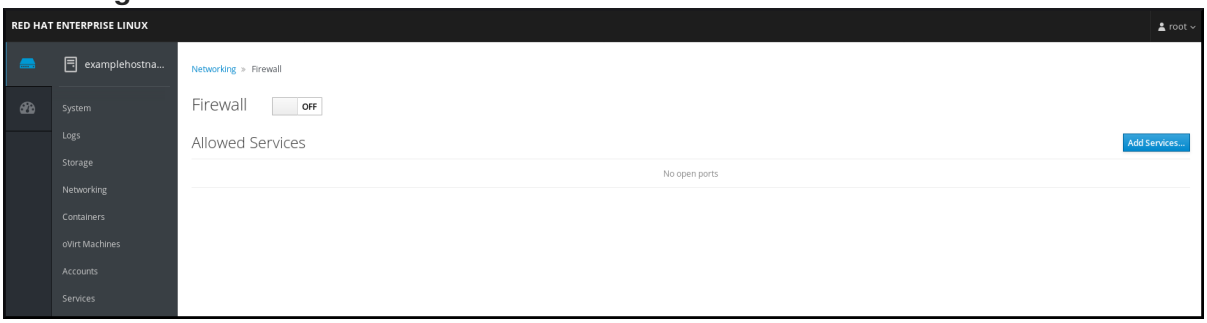
1.10.1.2. Gestión del cortafuegos en la consola web de RHEL 8

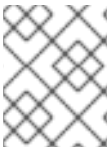
Para configurar el servicio **firewalld** en la consola web, navegue hasta **Red → Cortafuegos**.

Por defecto, el servicio **firewalld** está activado.

Procedimiento

1. Para activar o desactivar **firewalld** en la consola web, cambie el botón de alternancia **del cortafuegos**.





NOTA

Además, puede definir un acceso más detallado a través del cortafuegos a un servicio utilizando el botón **Añadir servicios**....

1.10.1.3. Recursos adicionales

- Para obtener información detallada sobre la configuración y el uso de un cortafuegos, consulte Uso y configuración de cortafuegos.

1.10.2. Gestión de la configuración básica de SELinux

Security-Enhanced Linux (SELinux) es una capa adicional de seguridad del sistema que determina qué procesos pueden acceder a qué archivos, directorios y puertos. Estos permisos se definen en las políticas de SELinux. Una política es un conjunto de reglas que guían el motor de seguridad de SELinux.

1.10.2.1. Estados y modos de SELinux

SELinux tiene dos estados posibles:

- Discapacitados
- Activado

Cuando SELinux está activado, se ejecuta en uno de los siguientes modos:

- Activado
  - Aplicación de
  - Permiso

En **enforcing mode**, SELinux aplica las políticas cargadas. SELinux deniega el acceso basándose en las reglas de las políticas de SELinux y habilita sólo las interacciones que están explícitamente permitidas. El modo Enforcing es el modo más seguro de SELinux y es el modo por defecto después de la instalación.

En **permissive mode**, SELinux no aplica las políticas cargadas. SELinux no niega el acceso, pero informa de las acciones que rompen las reglas al registro **/var/log/audit/audit.log**. El modo permisivo es el modo por defecto durante la instalación. El modo permisivo también es útil en algunos casos específicos, por ejemplo cuando se solucionan problemas.

Recursos adicionales

- Para más información sobre SELinux, consulte Uso de SELinux.

1.10.2.2. Garantizar el estado requerido de SELinux

Por defecto, SELinux funciona en modo reforzado. Sin embargo, en escenarios específicos, puedes poner SELinux en modo permisivo o incluso desactivarlo.

IMPORTANTE

Red Hat recomienda mantener su sistema en modo de refuerzo. Para propósitos de depuración, puede poner SELinux en modo permisivo.

Siga este procedimiento para cambiar el estado y el modo de SELinux en su sistema.

Procedimiento

1. Muestra el modo actual de SELinux:

```
$ getenforce
```

2. Para configurar temporalmente SELinux:

   a. Al modo de ejecución:

   ```
   # setenforce Enforcing
   ```

   b. A modo de permiso:

   ```
   # setenforce Permissive
   ```

NOTA

Después de reiniciar, el modo SELinux se establece en el valor especificado en el archivo de configuración **/etc/selinux/config**.

3. Para establecer que el modo SELinux persista a través de los reinicios, modifique la variable **SELINUX** en el archivo de configuración **/etc/selinux/config**.
   Por ejemplo, para cambiar SELinux al modo de refuerzo:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=enforcing
...
```

AVISO

Desactivar SELinux reduce la seguridad del sistema. Evite deshabilitar SELinux usando la opción **SELINUX=disabled** en el archivo **/etc/selinux/config** porque esto puede resultar en fugas de memoria y condiciones de carrera causando pánicos en el kernel. En su lugar, desactive SELinux añadiendo el parámetro **selinux=0** a la línea de comandos del kernel, tal y como se describe en Cambio de los modos de SELinux en el arranque.

Recursos adicionales

- Para más información sobre los cambios permanentes de los modos de SELinux, consulte Cambio de estados y modos de SELinux .

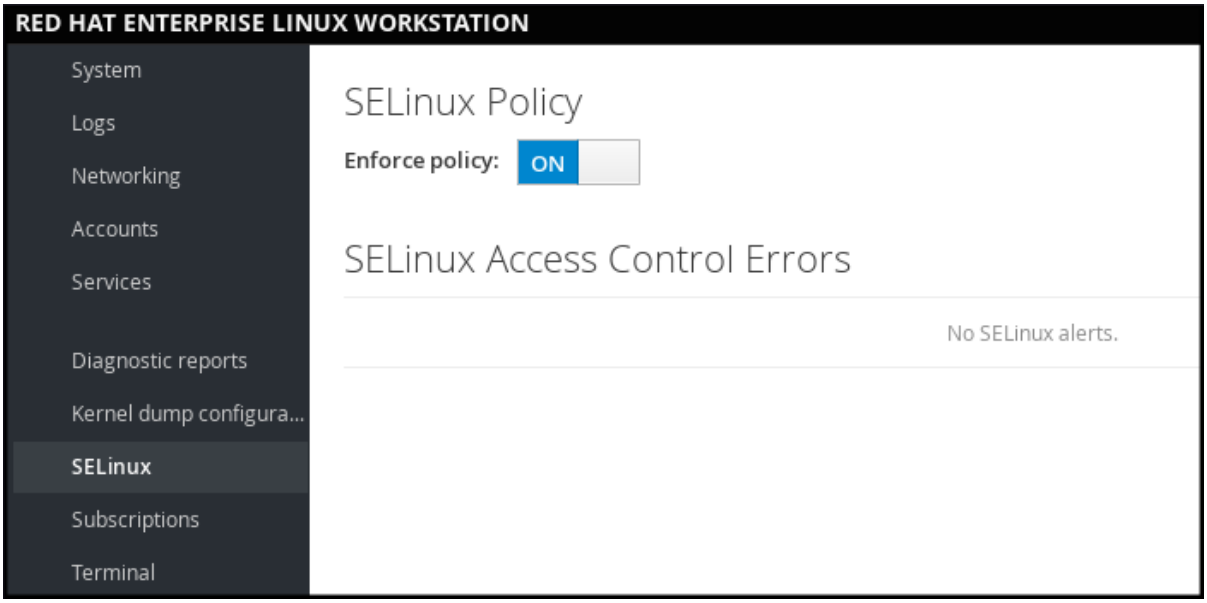
1.10.2.3. Cambiar los modos de SELinux en la consola web de RHEL 8

Puede configurar el modo SELinux a través de la consola web de RHEL 8 en el elemento de menú **SELinux**.

Por defecto, la política de aplicación de SELinux en la consola web está activada, y SELinux funciona en modo de aplicación. Al desactivarla, se cambia SELinux al modo permisivo. Tenga en cuenta que esta selección se revierte automáticamente en el siguiente arranque a la configuración definida en el archivo **/etc/sysconfig/selinux**.

Procedimiento

1. En la consola web, utilice el botón de conmutación de la **política de aplicación** en el elemento de menú SELinux para activar o desactivar la política de aplicación de SELinux.



1.10.2.4. Próximos pasos

- Puede gestionar varias personalizaciones locales de SELinux en varios sistemas de destino utilizando el rol de sistema **selinux**. Para más información, consulte la sección Desplegar la misma configuración de SELinux en varios sistemas.

1.10.3. Próximos pasos

- Uso de pares de claves en lugar de contraseñas para la autenticación SSH
- Endurecimiento de la seguridad
- Uso de SELinux
- Asegurar las redes

1.11. INTRODUCCIÓN A LA GESTIÓN DE CUENTAS DE USUARIO

Red Hat Enterprise Linux es un sistema operativo multiusuario, que permite a varios usuarios en diferentes ordenadores acceder a un único sistema instalado en una máquina.

Cada usuario opera bajo su propia cuenta, y la gestión de las cuentas de usuario representa por tanto un elemento central de la administración del sistema Red Hat Enterprise Linux.

1.11.1. Visión general de las cuentas y grupos de usuarios

Esta sección proporciona una visión general de las cuentas de usuario y los grupos. A continuación se presentan los diferentes tipos de cuentas de usuario:

- Cuentas de usuario normales:
  Las cuentas normales se crean para los usuarios de un determinado sistema. Estas cuentas pueden añadirse, eliminarse y modificarse durante la administración normal del sistema.

- Cuentas de usuario del sistema
  Las cuentas de usuario del sistema representan un identificador de aplicaciones particular en un sistema. Estas cuentas generalmente se añaden o manipulan sólo en el momento de la instalación del software, y no se modifican posteriormente.

  AVISO

  Se supone que las cuentas del sistema están disponibles localmente en un sistema. Si estas cuentas se configuran y se proporcionan de forma remota, como en el caso de una configuración LDAP, pueden producirse roturas del sistema y fallos en el inicio del servicio.

  Para las cuentas del sistema, los ID de usuario inferiores a 1000 están reservados. Para las cuentas normales, se pueden utilizar identificadores a partir de 1000. Sin embargo, la práctica recomendada es asignar ID a partir de 5000.

- Grupo
  Un grupo en una entidad que vincula varias cuentas de usuario con un propósito común, como la concesión de acceso a determinados archivos.

- Para más información, consulte

- Para asignar los identificadores, consulte el archivo **/etc/login.defs**.

1.11.2. Gestión de cuentas y grupos mediante herramientas de línea de comandos

Esta sección describe las herramientas básicas de la línea de comandos para gestionar las cuentas y los grupos de usuarios.

- Para mostrar las identificaciones de usuarios y grupos:

```
$ id
uid=1000(example.user) gid=1000(example.user) groups=1000(example.user),10(wheel)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

- Para crear una nueva cuenta de usuario:

```
# useradd example.user
```

- Para asignar una nueva contraseña a una cuenta de usuario perteneciente a *example.user*:

```
# passwd example.user
```

- Para añadir un usuario a un grupo:

```
# usermod -a -G example.group example.user
```

Recursos adicionales

- Las páginas de manual **useradd(8)**, **passwd(1)**, y **usermod(8)**.

1.11.3. Cuentas de usuario del sistema gestionadas en la consola web

Con las cuentas de usuario que se muestran en la consola web de RHEL se puede:

- Autenticar a los usuarios al acceder al sistema.
- Establezca los derechos de acceso al sistema.

La consola web de RHEL muestra todas las cuentas de usuario ubicadas en el sistema. Por lo tanto, puede ver al menos una cuenta de usuario justo después del primer inicio de sesión en la consola web.

Después de iniciar sesión en la consola web de RHEL, puede realizar las siguientes operaciones:

- Crear nuevas cuentas de usuario.
- Cambia sus parámetros.
- Bloquea las cuentas.
- Terminar las sesiones de los usuarios.

1.11.4. Añadir nuevas cuentas mediante la consola web

Siga los siguientes pasos para añadir cuentas de usuario al sistema y establecer los derechos de administración de las cuentas a través de la consola web de RHEL.

Requisitos previos

- La consola web de RHEL debe estar instalada y accesible. Para más detalles, consulte Instalación de la consola web.

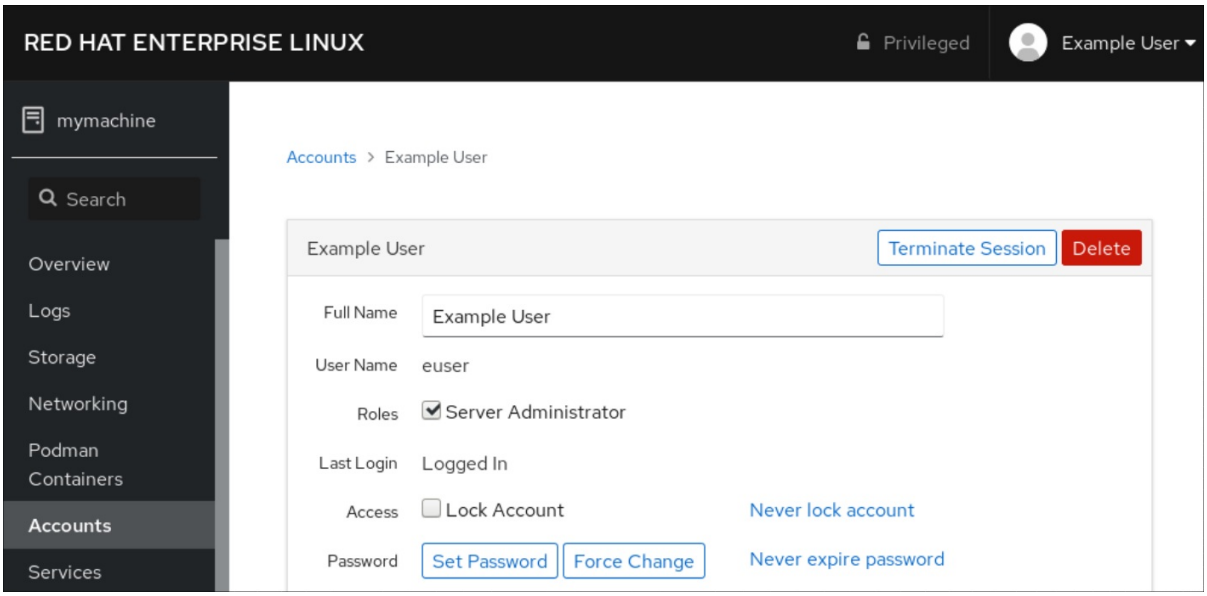
Procedimiento

1. Inicie sesión en la consola web de RHEL.
2. Haga clic en **Cuentas**.
3. Haga clic en **Crear una nueva cuenta**.

1. En el campo **Full Name**, introduzca el nombre completo del usuario.
   La consola web de RHEL sugiere automáticamente un nombre de usuario a partir del nombre completo y lo rellena en el campo **User Name**. Si no desea utilizar la convención de nomenclatura original que consiste en la primera letra del nombre y el apellido completo, actualice la sugerencia.

2. En los campos de **Password/Confirm**, introduzca la contraseña y vuelva a escribirla para verificar que es correcta.
   La barra de color situada debajo de los campos muestra el nivel de seguridad de la contraseña introducida, lo que no permite crear un usuario con una contraseña débil.

1. Haga clic en **Crear** para guardar la configuración y cerrar el cuadro de diálogo.
2. Seleccione la cuenta recién creada.
3. Seleccione **Server Administrator** en el elemento **Roles**.



Ahora puede ver la nueva cuenta en la configuración de **Accounts** y puede utilizar las credenciales para conectarse al sistema.

1.12. VOLCADO DE UN NÚCLEO ACCIDENTADO PARA SU POSTERIOR ANÁLISIS

Para analizar por qué se ha colgado un sistema, puede utilizar el servicio **kdump** para guardar el contenido de la memoria del sistema para su posterior análisis.

Esta sección proporciona una breve introducción a **kdump**, e información sobre la configuración de **kdump** usando la consola web de RHEL o usando el correspondiente rol de sistema de RHEL.

1.12.1. Qué es kdump

kdump es un servicio que proporciona un mecanismo de volcado de fallos. El servicio permite guardar el contenido de la memoria del sistema para su posterior análisis. **kdump** utiliza la llamada al sistema **kexec** para arrancar en el segundo núcleo (un *capture kernel*) sin reiniciar; y luego captura el contenido de la memoria del núcleo accidentado (un *crash dump* o un *vmcore*) y lo guarda. El segundo núcleo reside en una parte reservada de la memoria del sistema.

IMPORTANTE

Un volcado del kernel puede ser la única información disponible en caso de fallo del sistema (un error crítico). Por lo tanto, asegurarse de que **kdump** está operativo es importante en entornos de misión crítica. Red Hat aconseja que los administradores de sistemas actualicen y prueben regularmente **kexec-tools** en su ciclo normal de actualización del kernel. Esto es especialmente importante cuando se implementan nuevas características del kernel.

1.12.2. Configurar el uso de memoria de kdump y la ubicación del objetivo en la consola web

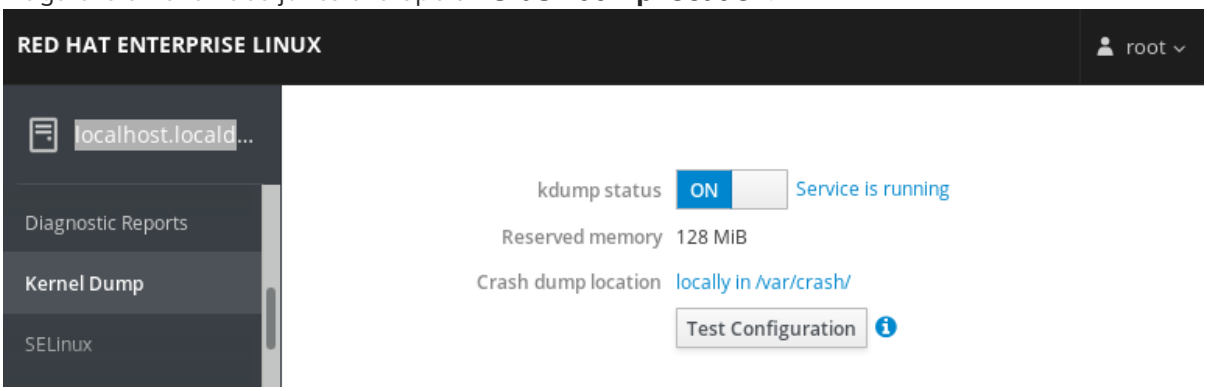
El procedimiento siguiente le muestra cómo utilizar la pestaña **Kernel Dump** en la interfaz de la consola web de Red Hat Enterprise Linux para configurar la cantidad de memoria que se reserva para el kernel kdump. El procedimiento también describe cómo especificar la ubicación de destino del archivo de volcado de vmcore y cómo probar su configuración.

Requisitos previos

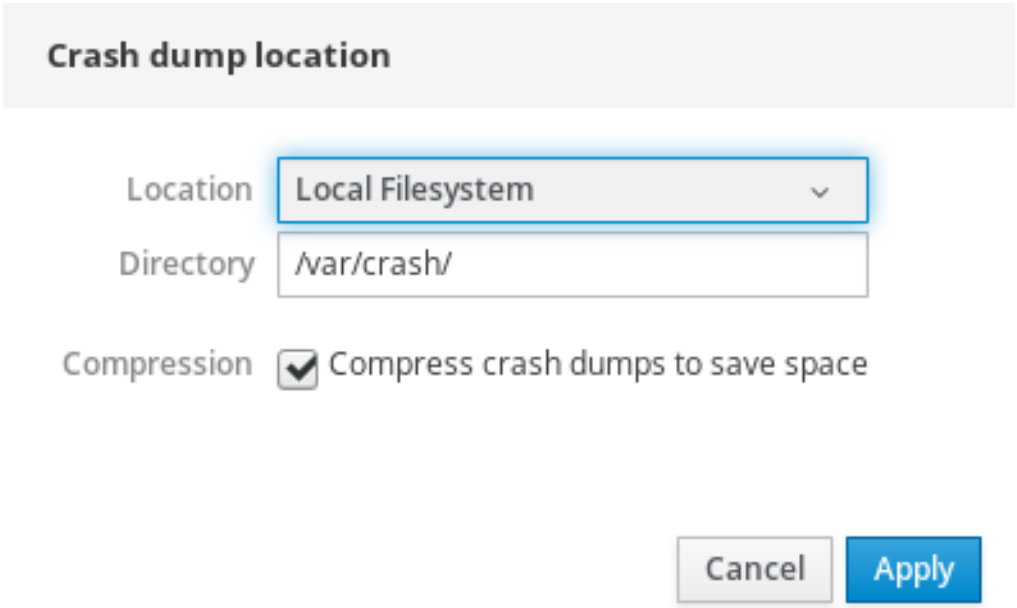
- Introducción al funcionamiento del *web console*

Procedimiento

1. Abra la pestaña **Kernel Dump** e inicie el servicio **kdump**.
2. Configure el uso de la memoria de **kdump** a través del *command line*.
3. Haga clic en el enlace junto a la opción **Crash dump location**.



4. Seleccione la opción **Local Filesystem** en el menú desplegable y especifique el directorio en el que desea guardar el volcado.

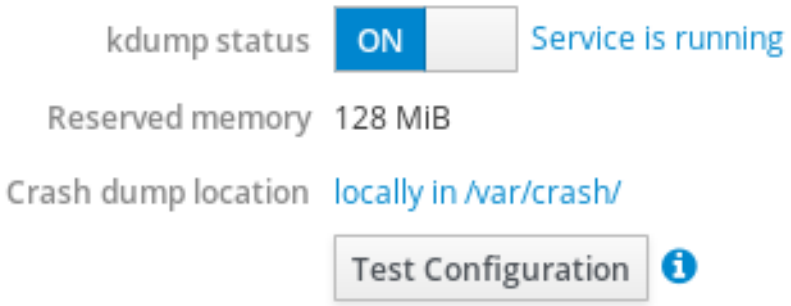


- Alternativamente, seleccione la opción **Remote over SSH** del menú desplegable para enviar el vmcore a una máquina remota utilizando el protocolo SSH.
  Rellene los campos **Server**, **ssh key**, y **Directory** con la dirección de la máquina remota, la ubicación de la clave ssh y un directorio de destino.
- Otra opción es seleccionar la opción **Remote over NFS** en el desplegable y rellenar el campo **Mount** para enviar el vmcore a una máquina remota utilizando el protocolo NFS.

NOTA

Marque la casilla **Compression** para reducir el tamaño del archivo vmcore.

5. Pruebe su configuración haciendo fallar el kernel.



AVISO

Este paso interrumpe la ejecución del kernel y provoca la caída del sistema y la pérdida de datos.

Recursos adicionales

- Para obtener una lista completa de los objetivos actualmente admitidos en **kdump**, consulte *Supported kdump targets* .
- Para obtener información sobre cómo configurar un servidor SSH y establecer una autenticación basada en claves, consulte *Using secure communications between two systems with OpenSSH*.

1.12.3. Configuración de kdump mediante los roles de sistema de RHEL

RHEL System Roles es una colección de roles y módulos de Ansible que proporcionan una interfaz de configuración consistente para gestionar remotamente múltiples sistemas RHEL. El rol **kdump** le permite configurar los parámetros básicos de volcado del kernel en varios sistemas.

AVISO

El rol **kdump** reemplaza la configuración **kdump** de los hosts administrados por completo, reemplazando el archivo **/etc/kdump.conf**. Además, si se aplica el rol **kdump**, también se reemplazan todas las configuraciones anteriores de **kdump**, aunque no estén especificadas por las variables del rol, reemplazando el archivo **/etc/sysconfig/kdump**.

El siguiente ejemplo de libro de jugadas muestra cómo aplicar el rol de sistema **kdump** para establecer la ubicación de los archivos de volcado de fallos:

```
---
- hosts: kdump-test
  vars:
    kdump_path: /var/crash
  roles:
    - rhel-system-roles.kdump
```

Recursos adicionales

- Para una referencia detallada sobre las variables de rol de **kdump**, instale el paquete **rhel-system-roles**, y vea los archivos **README.md** o **README.html** en el directorio **/usr/share/doc/rhel-system-roles/kdump**.
- Para obtener más información sobre las funciones del sistema RHEL, consulte Introducción a las funciones del sistema RHEL

1.12.4. Recursos adicionales

- Para obtener información más detallada sobre **kdump**, consulte Instalación y configuración de kdump.

1.13. RECUPERACIÓN Y RESTAURACIÓN DE UN SISTEMA

Para recuperar y restaurar un sistema utilizando una copia de seguridad existente, Red Hat Enterprise Linux proporciona la utilidad Relax-and-Recover (ReaR).

Puede utilizar la utilidad como solución de recuperación de desastres y también para la migración del sistema.

La utilidad le permite realizar las siguientes tareas:

- Producir una imagen de arranque y restaurar el sistema desde una copia de seguridad existente, utilizando la imagen.
- Replica la disposición original del almacén.
- Restaurar los archivos del usuario y del sistema.
- Restaurar el sistema en un hardware diferente.

Además, para la recuperación de desastres, también puede integrar cierto software de copia de seguridad con ReaR.

La configuración de ReaR implica los siguientes pasos de alto nivel:

1. Instalar ReaR.
2. Crear un sistema de rescate.
3. Modificar el archivo de configuración de ReaR, para añadir los detalles del método de copia de seguridad.

4. Generar archivos de copia de seguridad.

1.13.1. Configuración de ReaR

Siga los siguientes pasos para instalar los paquetes para utilizar la utilidad Relax-and-Recover (ReaR), crear un sistema de rescate, configurar y generar una copia de seguridad.

Requisitos previos

- Las configuraciones necesarias según el plan de restauración de la copia de seguridad están listas.
  Tenga en cuenta que puede utilizar el método de copia de seguridad **NETFS**, un método totalmente integrado e incorporado en ReaR.

Procedimiento

1. Instale ReaR, el programa de premasterización **genisomage**, y el paquete **syslinux** que proporciona un conjunto de cargadores de arranque:

```
# yum install rear genisoimage syslinux
```

2. Crear un sistema de rescate:

```
# rear mkrescue
```

3. Modifique el archivo de configuración de ReaR en un editor de su elección, por ejemplo:

```
# vi /etc/rear/local.conf
```

4. Añada los detalles de la configuración de la copia de seguridad a **/etc/rear/local.conf**. Por ejemplo, en el caso del método de copia de seguridad **NETFS**, añada las siguientes líneas:

```
BACKUP=NETFS
BACKUP_URL=backup.location
```

   Sustituya *backup.location* por la URL de la ubicación de su copia de seguridad.

5. Para configurar ReaR para que conserve los archivos de copia de seguridad anteriores cuando se creen los nuevos, añada también la siguiente línea al archivo de configuración:

```
NETFS_KEEP_OLD_BACKUP_COPY=y
```

6. Para que las copias de seguridad sean incrementales, es decir, que sólo se haga una copia de seguridad de los archivos modificados en cada ejecución, añada la siguiente línea:

```
BACKUP_TYPE=incremental
```

7. Realice una copia de seguridad según el plan de restauración.

1.14. SOLUCIÓN DE PROBLEMAS MEDIANTE ARCHIVOS DE REGISTRO

Los archivos de registro contienen mensajes sobre el sistema, incluyendo el kernel, los servicios y las

aplicaciones que se ejecutan en él. Contienen información que ayuda a solucionar problemas o a supervisar las funciones del sistema. El sistema de registro en Red Hat Enterprise Linux está basado en el protocolo incorporado **syslog**. Los programas particulares utilizan este sistema para registrar eventos y organizarlos en archivos de registro, los cuales son útiles cuando se audita el sistema operativo y se solucionan diversos problemas.

1.14.1. Servicios que gestionan los mensajes syslog

Los dos servicios siguientes gestionan los mensajes de **syslog**:

- El demonio **systemd-journald**
- El servicio **Rsyslog**

El demonio **systemd-journald** recoge los mensajes de varias fuentes y los reenvía a **Rsyslog** para su posterior procesamiento. El demonio **systemd-journald** recoge mensajes de las siguientes fuentes:

- Núcleo
- Primeras etapas del proceso de arranque
- Salida estándar y de error de los dæmons al iniciarse y ejecutarse
- **Syslog**

El servicio **Rsyslog** clasifica los mensajes de **syslog** por tipo y prioridad y los escribe en los archivos del directorio **/var/log**. El directorio **/var/log** almacena de forma persistente los mensajes de registro.

1.14.2. Subdirectorios de almacenamiento de mensajes syslog

Los siguientes subdirectorios bajo el directorio **/var/log** almacenan los mensajes de **syslog**.

- **/var/log/messages** - todos los mensajes de **syslog** excepto los siguientes
- **/var/log/secure** - mensajes y errores relacionados con la seguridad y la autenticación
- **/var/log/maillog** - mensajes y errores relacionados con el servidor de correo
- **/var/log/cron** - archivos de registro relacionados con tareas ejecutadas periódicamente
- **/var/log/boot.log** - archivos de registro relacionados con el inicio del sistema

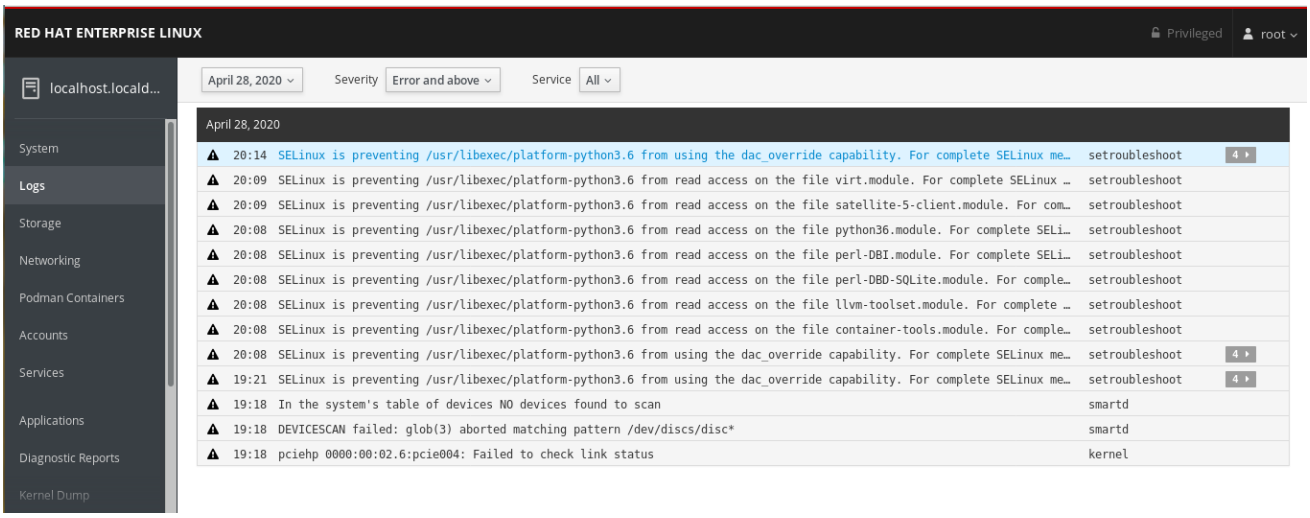
1.14.3. Inspección de los archivos de registro mediante la consola web

Siga los pasos de este procedimiento para inspeccionar los archivos de registro utilizando la consola web.

Procedimiento

1. Inicie sesión en la consola web de Red Hat Enterprise Linux 8.
   Para más detalles, consulte Iniciar sesión en la consola web .
2. Haga clic en **Logs**.

Figura 1.2. Inspección de los archivos de registro en la consola web de RHEL 8



1.14.4. Visualización de los registros mediante la línea de comandos

El Diario es un componente de systemd que ayuda a ver y gestionar los archivos de registro. Aborda los problemas relacionados con el registro tradicional, estrechamente integrado con el resto del sistema, y soporta varias tecnologías de registro y gestión de acceso para los archivos de registro.

Puede utilizar el comando **journalctl** para ver los mensajes en el diario del sistema utilizando la línea de comandos, por ejemplo:

```
$ journalctl -b | grep kvm
May 15 11:31:41 localhost.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
May 15 11:31:41 localhost.localdomain kernel: kvm-clock: cpu 0, msr 76401001, primary cpu clock
...
```

Tabla 1.1. Ver la información del sistema

Comando	Descripción
journalctl	Muestra todos los asientos recogidos.
journalctl FILEPATH	Muestra los registros relacionados con un archivo específico. Por ejemplo, el comando **journalctl /dev/sda** muestra los registros relacionados con el sistema de archivos **/dev/sda**.
journalctl -b	Muestra los registros del arranque actual.
journalctl -k -b -1	Muestra los registros del kernel para el arranque actual.

Tabla 1.2. Ver información sobre servicios específicos

Comando	Descripción

Comando	Descripción
journalctl -b _SYSTEMD_UNIT=foo	Filtra el registro para ver los que coinciden con el servicio "foo" **systemd**.
journalctl -b _SYSTEMD_UNIT=foo _PID=number	Combina las coincidencias. Por ejemplo, este comando muestra los registros de **systemd-units** que coinciden con **foo** y el PID **number**.
journalctl -b _SYSTEMD_UNIT=foo _PID=number _SYSTEMD_UNIT=foo1	El separador " " combina dos expresiones en un OR lógico. Por ejemplo, este comando muestra todos los mensajes del proceso del servicio **foo** con el **PID** más todos los mensajes del servicio **foo1** (de cualquiera de sus procesos).
journalctl -b _SYSTEMD_UNIT=foo _SYSTEMD_UNIT=foo1	Este comando muestra todas las entradas que coinciden con cualquiera de las dos expresiones, referidas al mismo campo. En este caso, este comando muestra los registros que coinciden con un systemd-unit **foo** o un systemd-unit **foo1**.

Tabla 1.3. Visualización de registros relacionados con botas específicas

Comando	Descripción
journalctl --list-boots	Muestra una lista tabular de los números de arranque, sus ID, y las marcas de tiempo del primer y último mensaje correspondiente al arranque. Puede utilizar el ID en el siguiente comando para ver información detallada.
journalctl --boot=ID _SYSTEMD_UNIT=foo	Muestra información sobre el ID de arranque especificado.

1.14.5. Recursos adicionales

- Para obtener más detalles sobre la configuración de **Rsyslog** para registrar registros, consulte Configuración de una solución de registro remoto .
- La página de manual **journalctl(1)**.
- Para más información sobre **systemd**, consulte Gestión de servicios con systemd .

1.15. ACCESO AL SOPORTE DE RED HAT

Esta sección describe cómo solucionar eficazmente sus problemas utilizando el soporte de Red Hat y **sosreport**.

Para obtener soporte de Red Hat, utilice el Portal del Cliente de Red Hat , que proporciona acceso a todo lo disponible con su suscripción.

1.15.1. Cómo obtener soporte de Red Hat a través del Portal del Cliente de Red Hat

La siguiente sección describe cómo utilizar el Portal del Cliente de Red Hat para obtener ayuda.

Requisitos previos

- Una cuenta de usuario válida en el Portal del Cliente de Red Hat. Consulte Crear un inicio de sesión de Red Hat.
- Una suscripción activa para el sistema RHEL.

Procedimiento

1. Acceda al soporte de Red Hat:
   a. Abra un nuevo caso de asistencia.
   b. Inicie un chat en vivo con un experto de Red Hat.
   c. Póngase en contacto con un experto de Red Hat llamando por teléfono o enviando un correo electrónico.

1.15.2. Solución de problemas con sosreport

El comando **sosreport** recoge detalles de configuración, información del sistema e información de diagnóstico de un sistema Red Hat Enterprise Linux.

La siguiente sección describe cómo utilizar el comando **sosreport** para producir informes para sus casos de soporte.

Requisitos previos

- Una cuenta de usuario válida en el Portal del Cliente de Red Hat. Consulte Crear un inicio de sesión de Red Hat.
- Una suscripción activa para el sistema RHEL.
- Un número de caso de apoyo.

Procedimiento

1. Instale el paquete **sos**:

```
# yum install sos
```

NOTA

La instalación mínima por defecto de Red Hat Enterprise Linux no incluye el paquete **sos**, que proporciona el comando **sosreport**.

2. Generar un informe:

```
# sosreport
```

3. Adjunte el informe a su caso de apoyo.
   Consulte el artículo ¿Cómo puedo adjuntar un archivo a un caso de soporte de Red Hat? Artículo de la Base de Conocimiento de Red Hat para más información.

   Tenga en cuenta que, al adjuntar el informe, se le pedirá que introduzca el número del caso de asistencia correspondiente.

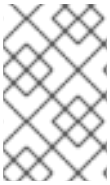
Recursos adicionales

- Para más información sobre **sosreport**, consulte el artículo ¿Qué es un sosreport y cómo crear uno en Red Hat Enterprise Linux 4.6 y posteriores? Artículo de Red Hat Knowledgebase.

CAPÍTULO 2. GESTIÓN DE PAQUETES DE SOFTWARE

2.1. HERRAMIENTAS DE GESTIÓN DE SOFTWARE EN RED HAT ENTERPRISE LINUX 8

En RHEL 8, la instalación de software está habilitada por la nueva versión de la herramienta **YUM** herramienta (**YUM v4**), que se basa en la **DNF** tecnología.



NOTA

La documentación de la fase previa identifica la tecnología como **DNF** y la herramienta se denomina **DNF** en la corriente ascendente. Como resultado, algunos resultados devueltos por la nueva **YUM** en RHEL 8 menciona **DNF**.

Aunque **YUM v4** utilizado en RHEL 8 está basado en **DNF**es compatible con **YUM v3** utilizado en RHEL 7. Para la instalación de software, el comando **yum** y la mayoría de sus opciones funcionan igual en RHEL 8 que en RHEL 7.

Algunos plug-ins y utilidades de **yum** los plug-ins y utilidades han sido portados al nuevo back end DNF, y pueden ser instalados con los mismos nombres que en RHEL 7. Los paquetes también proporcionan enlaces simbólicos de compatibilidad, por lo que los binarios, los archivos de configuración y los directorios pueden encontrarse en las ubicaciones habituales.

Tenga en cuenta que la antigua API de Python proporcionada por **YUM v3** ya no está disponible. Puede migrar sus plug-ins y scripts a la nueva API proporcionada por **YUM v4** (DNF Python API), que es estable y totalmente compatible. Consulte la Referencia de la API de DNF para obtener más información.

2.2. FLUJOS DE APLICACIÓN

Red Hat Enterprise Linux 8 introduce el concepto de Application Streams. Ahora se entregan y actualizan múltiples versiones de componentes del espacio de usuario con mayor frecuencia que los paquetes del sistema operativo principal. Esto proporciona una mayor flexibilidad para personalizar Red Hat Enterprise Linux sin afectar a la estabilidad subyacente de la plataforma o a implementaciones específicas.

Los componentes disponibles como Application Streams pueden ser empaquetados como módulos o paquetes RPM, y se entregan a través del repositorio AppStream en Red Hat Enterprise Linux 8. Cada Application Stream tiene un ciclo de vida determinado, ya sea el mismo que RHEL 8 o más corto, más adecuado a la aplicación particular. Los flujos de aplicaciones con un ciclo de vida más corto están listados en la página del ciclo de vida de los flujos de aplicaciones de Red Hat Enterprise Linux 8 .

Los módulos son colecciones de paquetes que representan una unidad lógica: una aplicación, una pila de lenguajes, una base de datos o un conjunto de herramientas. Estos paquetes se construyen, se prueban y se publican juntos.

Los flujos de módulos representan versiones de los componentes del flujo de aplicaciones. Por ejemplo, hay dos flujos (versiones) del servidor de base de datos PostgreSQL disponibles en el módulo postgresql: PostgreSQL 10 (el flujo por defecto) y PostgreSQL 9.6. Sólo se puede instalar un flujo del módulo en el sistema. Diferentes versiones pueden ser utilizadas en contenedores separados.

Los comandos detallados de los módulos se describen en el documento Instalación, gestión y eliminación de componentes del espacio de usuario. Para obtener una lista de los módulos disponibles en AppStream, consulte el manifiesto de paquetes.

2.3. BÚSQUEDA DE PAQUETES DE SOFTWARE

yum le permite realizar un conjunto completo de operaciones con paquetes de software.

La siguiente sección describe cómo utilizar **yum** para:

- Búsqueda de paquetes.
- Lista de paquetes.
- Lista de repositorios.
- Muestra información sobre los paquetes.
- Lista de grupos de paquetes.
- Especificar expresiones globales en la entrada de yum.

2.3.1. Búsqueda de paquetes con yum

- Para buscar un paquete, utilice:

```
# yum search term
```

  Sustituya *term* por un término relacionado con el paquete.

  Tenga en cuenta que el comando **yum search** devuelve coincidencias de términos dentro del nombre y el resumen de los paquetes. Esto hace que la búsqueda sea más rápida y le permite buscar paquetes de los que no conoce el nombre, pero de los que conoce un término relacionado.

- Para incluir coincidencias de términos en las descripciones de los paquetes, utilice:

```
# yum search --all term
```

  Sustituya *term* por el término que desee buscar en el nombre, el resumen o la descripción de un paquete.

  Tenga en cuenta que **yum search --all** permite una búsqueda más exhaustiva pero más lenta.

2.3.2. Listado de paquetes con yum

- Para listar la información de todos los paquetes instalados y disponibles, utilice:

```
# yum list --all
```

- Para listar todos los paquetes instalados en su sistema, utilice:

```
# yum list --installed
```

- Para listar todos los paquetes en todos los repositorios habilitados que están disponibles para instalar, utilice:

```
# yum list --available
```

Tenga en cuenta que puede filtrar los resultados añadiendo expresiones globales como argumentos. Consulte Sección 2.3.6, “Especificación de expresiones globales en la entrada de yum” para obtener más detalles.

2.3.3. Listado de repositorios con yum

- Para listar todos los repositorios habilitados en su sistema, utilice:

```
# yum repolist
```

- Para listar todos los repositorios deshabilitados en su sistema, utilice:

```
# yum repolist --disabled
```

- Para listar los repositorios habilitados y deshabilitados, utilice:

```
# yum repolist --all
```

- Para listar información adicional sobre los repositorios, utilice:

```
# yum repoinfo
```

Tenga en cuenta que puede filtrar los resultados pasando el ID o el nombre de los repositorios como argumentos o añadiendo expresiones globales. Consulte Sección 2.3.6, “Especificación de expresiones globales en la entrada de yum” para obtener más detalles.

2.3.4. Visualización de la información de los paquetes con yum

- Para mostrar información sobre uno o más paquetes, utilice:

```
# yum info package-name
```

  Sustituya *package-name* por el nombre del paquete.

Tenga en cuenta que puede filtrar los resultados añadiendo expresiones globales como argumentos. Consulte Sección 2.3.6, “Especificación de expresiones globales en la entrada de yum” para obtener más detalles.

2.3.5. Listado de grupos de paquetes con yum

- Para ver el número de grupos instalados y disponibles, utilice:

```
# yum group summary
```

- Para listar todos los grupos instalados y disponibles, utilice:

```
# yum group list
```

  Tenga en cuenta que puede filtrar los resultados añadiendo opciones de línea de comandos para el comando **yum group list** (**--hidden**, **--available**). Para ver más opciones disponibles, consulte las páginas del manual.

- Para listar los paquetes obligatorios y opcionales contenidos en un grupo determinado, utilice:

```
# yum group info group-name
```

  Sustituya *group-name* por el nombre del grupo.

Tenga en cuenta que puede filtrar los resultados añadiendo expresiones globales como argumentos. Consulte Sección 2.7.4, “Especificación de expresiones globales en la entrada de yum” para obtener más detalles.

2.3.6. Especificación de expresiones globales en la entrada de yum

los comandos**yum** permiten filtrar los resultados añadiendo uno o más *glob expressions* como argumentos. Las expresiones globales deben escaparse cuando se pasan como argumentos al comando **yum**. Para asegurarse de que las expresiones globales se pasen a **yum** como es debido, utilice uno de los siguientes métodos:

- Comillas dobles o simples en toda la expresión global.

```
# yum provides \ "*/file-name\ ~ - \ ~ -
```

  Sustituya *file-name* por el nombre del archivo.

- Escapa de los caracteres comodín precediéndolos de una barra invertida (\).

```
# yum provides \\Nde la que se puede obtener una copia de la mismafile-name
```

  Sustituya *file-name* por el nombre del archivo.

2.4. INSTALACIÓN DE PAQUETES DE SOFTWARE

La siguiente sección describe cómo utilizar **yum** para:

- Instalar paquetes.
- Instalar un grupo de paquetes.
- Especifica un nombre de paquete en la entrada de yum.

2.4.1. Instalación de paquetes con yum

- Para instalar un paquete y todas sus dependencias, utilice

```
# yum install package-name
```

  Sustituya *package-name* por el nombre del paquete.

- Para instalar varios paquetes y sus dependencias simultáneamente, utilice:

```
# yum install package-name-1 package-name-2
```

  Sustituya *package-name-1* y *package-name-2* por los nombres de los paquetes.

- Cuando se instalan paquetes en un sistema *multilib* (AMD64, máquina Intel 64), se puede especificar la arquitectura del paquete añadiéndola al nombre del mismo:

```
# yum install package-name.arch
```

  Sustituya *package-name.arch* por el nombre y la arquitectura del paquete.

- Si conoce el nombre del binario que desea instalar, pero no el nombre del paquete, puede utilizar la ruta del binario como argumento:

```
# yum install /usr/sbin/binary-file
```

  Sustituya ***/usr/sbin/binary-file*** por la ruta del archivo binario.

  yum busca en las listas de paquetes, encuentra el paquete que proporciona ***/usr/sbin/binary-file*** y le pregunta si quiere instalarlo.

- Para instalar un paquete previamente descargado desde un directorio local, utilice:

```
# yum install /path/
```

  Sustituya */path/* por la ruta del paquete.

Tenga en cuenta que puede optimizar la búsqueda de paquetes definiendo explícitamente cómo analizar el argumento. Consulte Sección 2.4.3, “Especificación de un nombre de paquete en la entrada de yum” para obtener más detalles.

2.4.2. Instalación de un grupo de paquetes con yum

- Para instalar un grupo de paquetes por un nombre de grupo, utilice:

```
# yum group install group-name
```

  O

```
# yum install @group-name
```

  Sustituya *group-name* por el nombre completo del grupo o colectivo ambiental.

- Para instalar un grupo de paquetes por el groupID, utilice:

```
# yum group install groupID
```

  Sustituya *groupID* por el ID del grupo.

2.4.3. Especificación de un nombre de paquete en la entrada de yum

Para optimizar el proceso de instalación y eliminación, puede añadir los sufijos **-n**, **-na**, o **-nerva** a los comandos **yum install** y **yum remove** para definir explícitamente cómo analizar un argumento:

- Para instalar un paquete utilizando su nombre exacto, utilice:

```
# yum install-n name
```

Sustituya *name* por el nombre exacto del paquete.

- Para instalar un paquete utilizando su nombre y arquitectura exactos, utilice:

```
# yum install-na name.architecture
```

Sustituya *name* y *architecture* por el nombre exacto y la arquitectura del paquete.

- Para instalar un paquete utilizando su nombre exacto, época, versión, lanzamiento y arquitectura, utilice:

```
# yum install-nevra name-epoch:version-release.architecture
```

Sustituya *name*, *epoch*, *version*, *release*, y *architecture* por el nombre exacto, la época, la versión, el lanzamiento y la arquitectura del paquete.

2.5. ACTUALIZACIÓN DE PAQUETES DE SOFTWARE

yum le permite comprobar si su sistema tiene alguna actualización pendiente. Puede listar los paquetes que necesitan ser actualizados y elegir actualizar un solo paquete, varios paquetes o todos los paquetes a la vez. Si alguno de los paquetes que elige actualizar tiene dependencias, también se actualizan.

La siguiente sección describe cómo utilizar **yum** para:

- Compruebe si hay actualizaciones.
- Actualizar un solo paquete.
- Actualizar un grupo de paquetes.
- Actualice todos los paquetes y sus dependencias.
- Aplique las actualizaciones de seguridad.
- Automatice las actualizaciones de software.

2.5.1. Comprobación de actualizaciones con yum

- Para ver qué paquetes instalados en su sistema tienen actualizaciones disponibles, utilice:

```
# yum check-update
```

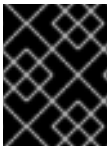
La salida devuelve la lista de paquetes y sus dependencias que tienen una actualización disponible.

2.5.2. Actualización de un solo paquete con yum

- Para actualizar un paquete, utilice:

```
# yum update package-name
```

Sustituya *package-name* por el nombre del paquete.



IMPORTANTE

Al aplicar actualizaciones al kernel, **yum** siempre **installs** un nuevo kernel, independientemente de si se utiliza el comando **yum update** o **yum install**.

2.5.3. Actualización de un grupo de paquetes con yum

- Para actualizar un grupo de paquetes, utilice:

```
# yum group update group-name
```

Sustituya *group-name* por el nombre del grupo de paquetes.

2.5.4. Actualizar todos los paquetes y sus dependencias con yum

- Para actualizar todos los paquetes y sus dependencias, utilice:

```
# yum update
```

2.5.5. Actualización de paquetes relacionados con la seguridad con yum

- Para actualizar a los últimos paquetes disponibles que tienen erratas de seguridad, utilice:

```
# yum update --security
```

- Para actualizar a los últimos paquetes de erratas de seguridad, utilice:

```
# yum update-minimal --security
```

2.5.6. Automatización de las actualizaciones de software

Para comprobar y descargar las actualizaciones de los paquetes de forma automática y periódica, puede utilizar la herramienta **DNF Automatic** que proporciona el paquete **dnf-automatic**.

DNF Automatic es una interfaz de línea de comandos alternativa a **yum** que es adecuada para la ejecución automática y regular utilizando temporizadores systemd, trabajos cron y otras herramientas similares.

DNF Automatic sincroniza los metadatos de los paquetes según sea necesario y luego comprueba si hay actualizaciones disponibles. Después, la herramienta puede realizar una de las siguientes acciones dependiendo de cómo se configure:

- Salir
- Descargue los paquetes actualizados
- Descargue y aplique las actualizaciones

El resultado de la operación se comunica a través de un mecanismo seleccionado, como la salida estándar o el correo electrónico.

2.5.6.1. Instalación del DNF automático

El siguiente procedimiento describe cómo instalar la herramienta **DNF Automatic**.

Procedimiento

- Para instalar el paquete **dnf-automatic**, utilice:

```
# yum install dnf-automatic
```

Pasos de verificación

- Para comprobar que la instalación se ha realizado correctamente, confirme la presencia del paquete **dnf-automatic** ejecutando el siguiente comando:

```
# rpm -qi dnf-automatic
```

2.5.6.2. DNF Archivo de configuración automática

Por defecto, **DNF Automatic** utiliza **/etc/dnf/automatic.conf** como archivo de configuración para definir su comportamiento.

El archivo de configuración se divide en las siguientes secciones temáticas:

- **[commands]** sección
  Establece el modo de funcionamiento de **DNF Automatic**.
- **[emitters]** sección
  Define cómo se informan los resultados de **DNF Automatic**.
- **[command_email]** sección
  Proporciona la configuración del emisor de correo electrónico para un comando externo utilizado para enviar correo electrónico.
- **[email]** sección
  Proporciona la configuración del emisor de correo electrónico.
- **[base]** sección
  Anula los ajustes del archivo de configuración principal de yum.

Con la configuración por defecto del archivo **/etc/dnf/automatic.conf**, **DNF Automatic** comprueba las actualizaciones disponibles, las descarga e informa de los resultados como salida estándar.

AVISO

Los ajustes del modo de funcionamiento de la sección **[commands]** son anulados por los ajustes utilizados por una unidad de temporización systemd para todas las unidades de temporización excepto **dnf-automatic.timer**.

Recursos adicionales

- Para más detalles sobre determinadas secciones, consulte la documentación de DNF Automatic.
- Para más detalles sobre las unidades de temporización de systemd, consulte las páginas del manual **man dnf-automatic**.
- Para conocer la visión general de las unidades de temporización de systemd incluidas en **dnf-automatic package**, consulte la sección 2.5.6.4 Visión general de las unidades de temporización de systemd incluidas en el paquete dnf-automatic

2.5.6.3. Activación del DNF automático

Para ejecutar **DNF Automatic**, siempre es necesario habilitar e iniciar una unidad de temporización específica de systemd. Puedes utilizar una de las unidades de temporización proporcionadas en el paquete **dnf-automatic**, o puedes escribir tu propia unidad de temporización dependiendo de tus necesidades.

La siguiente sección describe cómo habilitar **DNF Automatic**.

Requisitos previos

- Ha especificado el comportamiento de DNF Automático modificando el archivo de configuración **/etc/dnf/automatic.conf**.

Para más información sobre el archivo de configuración **DNF Automatic**, véase el apartado 2.5.6.2, "Archivo de configuración automática DNF".

Procedimiento

- Seleccione, habilite e inicie una unidad de temporizador systemd que se ajuste a sus necesidades:

```
# systemctl enable --now <unit>
```

  donde **<unit>** es uno de los siguientes temporizadores:

  - **dnf-automatic-download.timer**
  - **dnf-automatic-install.timer**
  - **dnf-automatic-notifyonly.timer**
  - **dnf-automatic.timer**

Para las actualizaciones disponibles en **downloading**, utilice:

```
# systemctl enable dnf-automatic-download.timer
```

```
# systemctl start dnf-automatic-download.timer
```

Para las actualizaciones disponibles en **downloading and installing**, utilice:

```
# systemctl enable dnf-automatic-install.timer
```

```
# systemctl start dnf-automatic-install.timer
```

Para **reporting** sobre las actualizaciones disponibles, utilice:

```
# systemctl enable dnf-automatic-notifyonly.timer
```

```
# systemctl start dnf-automatic-notifyonly.timer
```

Opcionalmente, se puede utilizar:

```
# systemctl enable dnf-automatic.timer
```

```
# systemctl start dnf-automatic.timer
```

En cuanto a la descarga y aplicación de actualizaciones, esta unidad de temporización se comporta de acuerdo con los ajustes del archivo de configuración **/etc/dnf/automatic.conf**. El comportamiento por defecto es similar al de **dnf-automatic-download.timer**: descarga los paquetes actualizados, pero no los instala.

NOTA

También puede ejecutar **DNF Automatic** ejecutando el archivo **/usr/bin/dnf-automatic** directamente desde la línea de comandos o desde un script personalizado.

Pasos de verificación

- Para comprobar que el temporizador está activado, ejecute el siguiente comando:

```
# systemctl status <systemd timer unit>
```

Recursos adicionales

- Para más información sobre los temporizadores dnf-automáticos, consulte las páginas del manual **man dnf-automatic**.
- Para obtener una visión general de las unidades de temporización de systemd incluidas en el paquete **dnf-automatic**, consulte la sección 2.5.6.4 Visión general de las unidades de temporización de systemd incluidas en el paquete **dnf-automatic**

2.5.6.4. Resumen de las unidades de temporización de systemd incluidas en el paquete dnf-automatic

Las unidades de tiempo de systemd tienen prioridad y anulan los ajustes del archivo de configuración **/etc/dnf/automatic.conf** en lo que respecta a la descarga y aplicación de actualizaciones.

Por ejemplo, si se establece:

download_updates = yes

en el archivo de configuración de **/etc/dnf/automatic.conf**, pero ha activado la unidad **dnf-automatic-notifyonly.timer**, los paquetes no se descargarán.

El paquete **dnf-automatic** incluye las siguientes unidades de temporización systemd:

Unidad de temporizador	Función	¿Anula los ajustes del archivo **/etc/dnf/automatic.conf**?
dnf-automatic-download.timer	Descarga los paquetes a la caché y los pone a disposición para su actualización. Nota: Esta unidad de temporización no instala los paquetes actualizados. Para realizar la instalación, debe ejecutar el comando **dnf update**.	Sí
dnf-automatic-install.timer	Descarga e instala los paquetes actualizados.	Sí
dnf-automatic-notifyonly.timer	Descarga sólo los datos del repositorio para mantener la caché del mismo al día y le notifica las actualizaciones disponibles. Nota: Este temporizador no descarga ni instala los paquetes actualizados	Sí
dnf-automatic.timer	El comportamiento de este temporizador en lo que respecta a la descarga y aplicación de actualizaciones se especifica mediante los ajustes del archivo de configuración **/etc/dnf/automatic.conf**. El comportamiento por defecto es el mismo que el de la unidad **dnf-automatic-download.timer**: sólo descarga los paquetes, pero no los instala.	No

Recursos adicionales

- Para más información sobre los temporizadores de **dnf-automatic**, consulte las páginas del manual **man dnf-automatic**.
- Para más información sobre el archivo de configuración **/etc/dnf/automatic.conf**, véase el apartado 2.5.6.2. Archivo de configuración automática DNF

2.6. DESINSTALACIÓN DE PAQUETES DE SOFTWARE

La siguiente sección describe cómo utilizar **yum** para:

- Retire los paquetes.

- Eliminar un grupo de paquetes.
- Especifica un nombre de paquete en la entrada de yum.

2.6.1. Eliminación de paquetes con yum

- Para eliminar un paquete concreto y todos los paquetes dependientes, utilice:

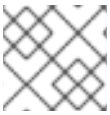
```
# yum remove package-name
```

Sustituya *package-name* por el nombre del paquete.

- Para eliminar varios paquetes y sus dependencias simultáneamente, utilice:

```
# yum remove package-name-1 package-name-2
```

Sustituya *package-name-1* y *package-name-2* por los nombres de los paquetes.



NOTA

yum no puede eliminar un paquete sin eliminar los paquetes dependientes.

Tenga en cuenta que puede optimizar la búsqueda de paquetes definiendo explícitamente cómo analizar el argumento. Consulte Sección 2.6.3, "Especificación de un nombre de paquete en la entrada de yum" para obtener más detalles.

2.6.2. Eliminar un grupo de paquetes con yum

- Para eliminar un grupo de paquetes por el nombre del grupo, utilice:

```
# yum group remove group-name
```

O

```
# yum remove @group-name
```

Sustituya *group-name* por el nombre completo del grupo.

- Para eliminar un grupo de paquetes por el groupID, utilice:

```
# yum group remove groupID
```

Sustituya *groupID* por el ID del grupo.

2.6.3. Especificación de un nombre de paquete en la entrada de yum

Para optimizar el proceso de instalación y eliminación, puede añadir los sufijos **-n**, **-na**, o **-nerva** a los comandos **yum install** y **yum remove** para definir explícitamente cómo analizar un argumento:

- Para instalar un paquete utilizando su nombre exacto, utilice:

```
# yum install-n name
```

Sustituya *name* por el nombre exacto del paquete.

- Para instalar un paquete utilizando su nombre y arquitectura exactos, utilice:

```
# yum install-na name.architecture
```

Sustituya *name* y *architecture* por el nombre exacto y la arquitectura del paquete.

- Para instalar un paquete utilizando su nombre exacto, época, versión, lanzamiento y arquitectura, utilice:

```
# yum install-nevra name-epoch:version-release.architecture
```

Sustituya *name*, *epoch*, *version*, *release*, y *architecture* por el nombre exacto, la época, la versión, el lanzamiento y la arquitectura del paquete.

2.7. GESTIÓN DE GRUPOS DE PAQUETES DE SOFTWARE

Un grupo de paquetes es una colección de paquetes que tienen un propósito común (**System Tools**, **Sound and Video**). Al instalar un grupo de paquetes se extrae un conjunto de paquetes dependientes, lo que ahorra mucho tiempo.

La siguiente sección describe cómo utilizar **yum** para:

- Lista de grupos de paquetes.
- Instalar un grupo de paquetes.
- Eliminar un grupo de paquetes.
- Especificar expresiones globales en la entrada de yum.

2.7.1. Listado de grupos de paquetes con yum

- Para ver el número de grupos instalados y disponibles, utilice:

```
# yum group summary
```

- Para listar todos los grupos instalados y disponibles, utilice:

```
# yum group list
```

Tenga en cuenta que puede filtrar los resultados añadiendo opciones de línea de comandos para el comando **yum group list** (**--hidden**, **--available**). Para ver más opciones disponibles, consulte las páginas del manual.

- Para listar los paquetes obligatorios y opcionales contenidos en un grupo determinado, utilice:

```
# yum group info group-name
```

Sustituya *group-name* por el nombre del grupo.

Tenga en cuenta que puede filtrar los resultados añadiendo expresiones globales como argumentos. Consulte Sección 2.7.4, “Especificación de expresiones globales en la entrada de yum” para obtener más detalles.

2.7.2. Instalación de un grupo de paquetes con yum

- Para instalar un grupo de paquetes por un nombre de grupo, utilice:

```
# yum group install group-name
```

O

```
# yum install @group-name
```

Sustituya *group-name* por el nombre completo del grupo o colectivo ambiental.

- Para instalar un grupo de paquetes por el groupID, utilice:

```
# yum group install groupID
```

Sustituya *groupID* por el ID del grupo.

2.7.3. Eliminar un grupo de paquetes con yum

- Para eliminar un grupo de paquetes por el nombre del grupo, utilice:

```
# yum group remove group-name
```

O

```
# yum remove @group-name
```

Sustituya *group-name* por el nombre completo del grupo.

- Para eliminar un grupo de paquetes por el groupID, utilice:

```
# yum group remove groupID
```

Sustituya *groupID* por el ID del grupo.

2.7.4. Especificación de expresiones globales en la entrada de yum

los comandos**yum** permiten filtrar los resultados añadiendo uno o más *glob expressions* como argumentos. Las expresiones globales deben escaparse cuando se pasan como argumentos al comando **yum**. Para asegurarse de que las expresiones globales se pasen a **yum** como es debido, utilice uno de los siguientes métodos:

- Comillas dobles o simples en toda la expresión global.

```
# yum provides \ "*/file-name\ ~ - \ ~ -
```

Sustituya *file-name* por el nombre del archivo.

- Escapa de los caracteres comodín precediéndolos de una barra invertida (\).

```
# yum provides \\Nde la que se puede obtener una copia de la misma file-name
```

Sustituya *file-name* por el nombre del archivo.

2.8. MANEJO DEL HISTORIAL DE GESTIÓN DE PAQUETES

El comando **yum history** permite revisar la información sobre la línea de tiempo de **yum** transacciones, las fechas y horas en que ocurrieron, el número de paquetes afectados, si estas transacciones tuvieron éxito o fueron abortadas, y si la base de datos RPM fue modificada entre las transacciones. **yum history** comando también puede ser utilizado para deshacer o rehacer las transacciones.

La siguiente sección describe cómo utilizar **yum** para:

- Lista de transacciones.
- Revertir las transacciones.
- Transacciones repetidas.
- Especificar expresiones globales en la entrada de yum.

2.8.1. Listado de transacciones con yum

- Para mostrar una lista de todas las últimas **yum** transacciones, utilice:

```
# yum history
```

- Para mostrar una lista de todas las últimas operaciones de un paquete seleccionado, utilice:

```
# yum history list package-name
```

Sustituya *package-name* por el nombre del paquete. Puede filtrar la salida del comando añadiendo expresiones globales. Consulte Sección 2.8.4, “Especificación de expresiones globales en la entrada de yum” para obtener más detalles.

- Para examinar una transacción concreta, utilice:

```
# yum history info transactionID
```

Sustituya *transactionID* por el ID de la transacción.

2.8.2. Revertir transacciones con yum

- Para revertir una operación concreta, utilice:

```
# yum history undo transactionID
```

Sustituya *transactionID* por el ID de la transacción.

- Para revertir la última transacción, utilice:

```
# yum history undo last
```

Tenga en cuenta que el comando **yum history undo** sólo revierte los pasos que se realizaron durante la transacción. Si la transacción instaló un nuevo paquete, el comando **yum history undo** lo desinstala. Si la transacción desinstaló un paquete, el comando **yum history undo** lo reinstala. **yum history undo** también intenta degradar todos los paquetes actualizados a sus versiones anteriores, si los paquetes más antiguos aún están disponibles.

2.8.3. Repetición de operaciones con yum

- Para repetir una operación concreta, utilice:

```
# yum history redo transactionID
```

  Sustituya *transactionID* por el ID de la transacción.

- Para repetir la última transacción, utilice:

```
# yum history redo last
```

Tenga en cuenta que el comando **yum history redo** sólo repite los pasos que se realizaron durante la transacción.

2.8.4. Especificación de expresiones globales en la entrada de yum

los comandos**yum** permiten filtrar los resultados añadiendo uno o más *glob expressions* como argumentos. Las expresiones globales deben escaparse cuando se pasan como argumentos al comando **yum**. Para asegurarse de que las expresiones globales se pasen a **yum** como es debido, utilice uno de los siguientes métodos:

- Comillas dobles o simples en toda la expresión global.

```
# yum provides \ "*/file-name\ ~ - \ ~ -
```

  Sustituya *file-name* por el nombre del archivo.

- Escapa de los caracteres comodín precediéndolos de una barra invertida (\).

```
# yum provides \\Nde la que se puede obtener una copia de la mismafile-name
```

  Sustituya *file-name* por el nombre del archivo.

2.9. GESTIÓN DE REPOSITORIOS DE SOFTWARE

La información de configuración de **yum** y las utilidades relacionadas se almacenan en el archivo **/etc/yum.conf**. Este archivo contiene una o varias **[*repository*]** secciones, que le permiten establecer opciones específicas del repositorio.

Se recomienda definir los repositorios individuales en los archivos **.repo** nuevos o existentes en el directorio **/etc/yum.repos.d/**.

Tenga en cuenta que los valores que defina en las secciones individuales de **[*repository*]** del archivo **/etc/yum.conf** anulan los valores definidos en la sección **[main]**.

La siguiente sección describe cómo:

- Establezca **[*repository*]** opciones.
- Añade un **yum** repositorio.
- Habilitar un **yum** repositorio.
- Desactivar un **yum** repositorio.

2.9.1. Configuración de las opciones del repositorio yum

El archivo de configuración **/etc/yum.conf** contiene las secciones **[*repository*]** donde *repository* es un ID de repositorio único. Las secciones **[*repository*]** secciones le permiten definir repositorios **yum** repositorios individuales.

NOTA

No dé a los repositorios personalizados nombres utilizados por los repositorios de Red Hat para evitar conflictos.

Para una lista completa de las opciones **[*repository*]** opciones, consulte la sección **[*repository*] OPTIONS** de la página del manual **yum.conf**(5).

2.9.2. Añadir un repositorio yum

Para definir un nuevo repositorio, puede:

- Añada una **[*repository*]** sección en el archivo **/etc/yum.conf**.
- Añada una **[*repository*]** sección a un archivo **.repo** en el directorio **/etc/yum.repos.d/**. **yum** los repositorios suelen proporcionar su propio archivo **.repo**.

NOTA

Se recomienda definir los repositorios en un archivo **.repo** en lugar de **/etc/yum.conf** ya que todos los archivos con la extensión **.repo** en este directorio son leídos por **yum**.

- Para añadir un repositorio a su sistema y habilitarlo, utilice:

```
# yum-config-manager --add-repo repository_URL
```

Sustituya *repository_url* por la URL que apunta al repositorio.

AVISO

La obtención e instalación de paquetes de software de fuentes no verificadas o no confiables que no sean las de Red Hat basadas en certificados **Content Delivery Network** (CDN) constituye un riesgo potencial para la seguridad y podría conducir a problemas de seguridad, estabilidad, compatibilidad y mantenimiento.

2.9.3. Habilitación de un repositorio yum

- Para habilitar un repositorio, utilice:

```
# yum-config-manager --enable repositoryID
```

Sustituya *repositoryID* por el identificador único del repositorio.

Para ver la lista de IDs de repositorios disponibles, consulte Sección 2.3.2, “Listado de paquetes con yum”.

2.9.4. Desactivación de un repositorio yum

- Para desactivar un repositorio yum, utilice:

```
# yum-config-manager --disable repositoryID
```

Sustituya *repositoryID* por el identificador único del repositorio.

Para ver la lista de IDs de repositorios disponibles, consulte Sección 2.3.2, “Listado de paquetes con yum”.

2.10. CONFIGURACIÓN DE YUM

La información de configuración de **yum** y las utilidades relacionadas se almacenan en el archivo **/etc/yum.conf**. Este archivo contiene una sección obligatoria **[main]**, que permite establecer opciones **yum** que tienen efecto global.

La siguiente sección describe cómo:

- Vea las configuraciones actuales de **yum**.
- Establezca las opciones de **yum** [main].
- Utilice los complementos de **yum**.

2.10.1. Ver las configuraciones actuales de yum

- Para mostrar los valores actuales de las opciones globales de yum especificadas en la sección **[main]** del archivo **/etc/yum.conf**, utilice:

```
# yum config-manager --dump
```

2.10.2. Configuración de las opciones principales de yum

El archivo de configuración **/etc/yum.conf** contiene una sección **[main]**. Los pares clave-valor de esta sección afectan a cómo **yum** opera y trata los repositorios.

Puede añadir opciones adicionales en el apartado **[main]** en **/etc/yum.conf**.

Para obtener una lista completa de las opciones disponibles en **[main]**, consulte la sección **[main] OPTIONS** de la página del manual **yum.conf**(5).

2.10.3. Uso de los plug-ins de yum

yum proporciona plug-ins que amplían y mejoran su funcionamiento. Algunos complementos se instalan por defecto.

La siguiente sección describe cómo activar, configurar y desactivar **yum** plug-ins.

2.10.3.1. Gestión de los plug-ins de yum

Los archivos de configuración de los complementos siempre contienen una sección **[main]** en la que la opción **enabled=** controla si el complemento se activa cuando se ejecutan los comandos **yum**. Si falta esta opción, puedes añadirla manualmente al archivo.

Cada plug-in instalado tiene su propio archivo de configuración en el directorio **/etc/dnf/plugins/**. En estos archivos se pueden activar o desactivar las opciones específicas del plug-in.

2.10.3.2. Activación de los plug-ins de yum

- Para habilitar todos los plug-ins de yum:

  1. Asegúrese de que haya una línea que empiece por **plugins=** en la sección **[main]** del archivo **/etc/yum.conf**.

  2. Ajuste el valor de **plugins=** a **1**.

     ```
     plugins=1
     ```

2.10.3.3. Desactivación de los plug-ins de yum

- Para desactivar todos los complementos de yum:

  1. Asegúrese de que haya una línea que empiece por **plugins=** en la sección **[main]** del archivo **/etc/yum.conf**.

  2. Ajuste el valor de **plugins=** a **0**.

     ```
     plugins=0
     ```

IMPORTANTE

Se aconseja desactivar todos los plug-ins en **not**. Algunos plug-ins proporcionan importantes servicios de yum. En particular, los plugins **product-id** y **subscription-manager** proporcionan soporte para el certificado basado en **Content Delivery Network** (**CDN**). Desactivar los plug-ins globalmente se proporciona como una opción de conveniencia, y es aconsejable sólo cuando se diagnostica un problema potencial con **yum**.

- Para desactivar todos los complementos de yum para un comando en particular, añada la opción **--noplugins** al comando.

  ```
  # yum --noplugins update
  ```

- Para desactivar ciertos complementos de yum para un solo comando, añada la opción **--disableplugin=*plugin-name*** al comando.

```
# yum update --disableplugin=plugin-name
```

Sustituya *plugin-name* por el nombre del complemento.

CAPÍTULO 3. GESTIÓN DE SERVICIOS CON SYSTEMD

3.1. INTRODUCCIÓN A SYSTEMD

Systemd es un gestor de sistemas y servicios para sistemas operativos Linux. Está diseñado para ser compatible con los scripts de inicio de SysV, y proporciona una serie de características tales como el inicio paralelo de los servicios del sistema en el momento del arranque, la activación bajo demanda de los demonios, o la lógica de control de servicios basada en la dependencia. A partir de Red Hat Enterprise Linux 7, **systemd** reemplazó a Upstart como el sistema de inicio por defecto.

Systemd introduce el concepto de *systemd units*. Estas unidades están representadas por archivos de configuración de unidades ubicados en uno de los directorios enumerados en la siguiente tabla.

Tabla 3.1. Ubicación de los archivos de la unidad Systemd

Directorio	Descripción
/usr/lib/systemd/system/	Archivos de unidad Systemd distribuidos con los paquetes RPM instalados.
/run/systemd/system/	Archivos de unidad Systemd creados en tiempo de ejecución. Este directorio tiene prioridad sobre el directorio con los archivos de unidad de servicio instalados.
/etc/systemd/system/	Los archivos de unidad de Systemd creados por **systemctl enable**, así como los archivos de unidad añadidos para ampliar un servicio. Este directorio tiene prioridad sobre el directorio con los archivos de unidad en tiempo de ejecución.

Las unidades encapsulan información sobre:

- Servicios del sistema
- Tomas de corriente para escuchar
- Otros objetos relevantes para el sistema init

Para obtener una lista completa de los tipos de unidades systemd disponibles, consulte la siguiente tabla.

Tabla 3.2. Tipos de unidades systemd disponibles

Tipo de unidad	Extensión del archivo	Descripción
Unidad de servicio	**.service**	Un servicio del sistema.
Unidad de destino	**.target**	Un grupo de unidades systemd.

Tipo de unidad	Extensión del archivo	Descripción
Unidad de montaje automático	**.automount**	Un punto de montaje automático del sistema de archivos.
Unidad de dispositivo	**.device**	Un archivo de dispositivo reconocido por el kernel.
Montar la unidad	**.mount**	Un punto de montaje del sistema de archivos.
Unidad de ruta	**.path**	Un archivo o directorio en un sistema de archivos.
Unidad de alcance	**.scope**	Un proceso creado externamente.
Unidad de corte	**.slice**	Un grupo de unidades organizadas jerárquicamente que gestionan los procesos del sistema.
Unidad de enchufe	**.socket**	Un socket de comunicación entre procesos.
Unidad de intercambio	**.swap**	Un dispositivo de intercambio o un archivo de intercambio.
Unidad de temporizador	**.timer**	Un temporizador systemd.

Anulando la configuración por defecto de systemd mediante system.conf
La configuración por defecto de **systemd** se define durante la compilación y se puede encontrar en el archivo de configuración de systemd en **/etc/systemd/system.conf**. Utilice este archivo si desea desviarse de esos valores predeterminados y anular los valores predeterminados seleccionados para las unidades de systemd de forma global.

Por ejemplo, para anular el valor por defecto del límite de tiempo de espera, que está fijado en 90 segundos, utilice el parámetro **DefaultTimeoutStartSec** para introducir el valor requerido en segundos.

```
DefaultTimeoutStartSec=required value
```

Para más información, consulte Ejemplo 3.11, “Cambiar el límite de tiempo de espera” .

3.1.1. Características principales

El sistema systemd y el gestor de servicios proporcionan las siguientes características principales:

- **Socket-based activation** - En el momento del arranque, **systemd** crea sockets de escucha para todos los servicios del sistema que soportan este tipo de activación, y pasa los sockets a estos servicios tan pronto como se inician. Esto no sólo permite **systemd** iniciar servicios en

paralelo, sino que también hace posible reiniciar un servicio sin perder ningún mensaje enviado a él mientras no está disponible: el socket correspondiente sigue siendo accesible y todos los mensajes se ponen en cola.
Systemd utiliza *socket units* para la activación basada en sockets.

- **Bus-based activation** - Los servicios del sistema que utilizan D-Bus para la comunicación entre procesos pueden iniciarse bajo demanda la primera vez que una aplicación cliente intenta comunicarse con ellos **Systemd** utiliza *D-Bus service files* para la activación basada en el bus.

- **Device-based activation** - Los servicios del sistema que admiten la activación basada en dispositivos pueden iniciarse a petición cuando se conecta un tipo concreto de hardware o está disponible **Systemd** utiliza *device units* para la activación basada en dispositivos.

- **Path-based activation** - Los servicios del sistema que soportan la activación basada en la ruta pueden iniciarse bajo demanda cuando un archivo o directorio concreto cambia de estado **Systemd** utiliza *path units* para la activación basada en la ruta.

- **Mount and automount point management** - **Systemd** controla y gestiona los puntos de montaje y automontaje **Systemd** utiliza *mount units* para los puntos de montaje y *automount units* para los puntos de automontaje.

- **Aggressive parallelization** - Debido al uso de la activación basada en sockets, **systemd** puede iniciar los servicios del sistema en paralelo tan pronto como todos los sockets de escucha están en su lugar. En combinación con los servicios del sistema que soportan la activación bajo demanda, la activación en paralelo reduce significativamente el tiempo necesario para arrancar el sistema.

- **Transactional unit activation logic** - Antes de activar o desactivar una unidad, **systemd** calcula sus dependencias, crea una transacción temporal y verifica que esta transacción sea consistente. Si una transacción es inconsistente **systemd** intenta automáticamente corregirla y eliminar de ella los trabajos no esenciales antes de informar de un error.

- **Backwards compatibility with SysV init** - **Systemd** soporta los scripts de init de SysV como se describe en el *Linux Standard Base Core Specification* lo que facilita la ruta de actualización de las unidades de servicio systemd.

3.1.2. Cambios de compatibilidad

El sistema systemd y el gestor de servicios están diseñados para ser mayormente compatibles con SysV init y Upstart. Los siguientes son los cambios de compatibilidad más notables con respecto al sistema Red Hat Enterprise Linux 6 que utilizaba SysV init:

- **Systemd** sólo tiene un soporte limitado para los niveles de ejecución. Proporciona una serie de unidades de destino que se pueden asignar directamente a estos niveles de ejecución y, por razones de compatibilidad, también se distribuye con el comando anterior **runlevel**. Sin embargo, no todos los objetivos de systemd pueden ser asignados directamente a niveles de ejecución, y como consecuencia, este comando puede devolver **N** para indicar un nivel de ejecución desconocido. Se recomienda evitar el uso del comando **runlevel** si es posible. Para obtener más información sobre los objetivos de systemd y su comparación con los niveles de ejecución, consulte Sección 3.3, “Trabajar con objetivos systemd” .

- La utilidad **systemctl** no admite comandos personalizados. Además de los comandos estándar como **start**, **stop**, y **status**, los autores de los scripts de init de SysV podrían implementar soporte para cualquier número de comandos arbitrarios con el fin de proporcionar funcionalidad adicional. Por ejemplo, el script de init para **iptables** podría ser ejecutado con el comando

panic, que inmediatamente activaría el modo de pánico y reconfiguraría el sistema para comenzar a dejar caer todos los paquetes entrantes y salientes. Esto no está soportado en **systemd** y el **systemctl** sólo acepta comandos documentados.
Para más información sobre la utilidad **systemctl** y su comparación con la anterior **service**, consulte Tabla 3.3, "Comparación de la utilidad de servicio con systemctl" .

- La utilidad **systemctl** no se comunica con los servicios que no han sido iniciados por **systemd**. Cuando **systemd** inicia un servicio del sistema, almacena el ID de su proceso principal para poder seguirlo. La utilidad **systemctl** utiliza entonces este PID para consultar y gestionar el servicio. En consecuencia, si un usuario inicia un demonio concreto directamente en la línea de comandos, **systemctl** no puede determinar su estado actual ni detenerlo.

- **Systemd** detiene sólo los servicios en ejecución. Anteriormente, cuando se iniciaba la secuencia de apagado, Red Hat Enterprise Linux 6 y las versiones anteriores del sistema utilizaban enlaces simbólicos ubicados en el directorio **/etc/rc0.d/** para detener todos los servicios del sistema disponibles, independientemente de su estado. Con **systemd** sólo se detienen los servicios en ejecución al apagar el sistema.

- Los servicios del sistema no pueden leer del flujo de entrada estándar. Cuando **systemd** inicia un servicio, conecta su entrada estándar a **/dev/null** para evitar cualquier interacción con el usuario.

- Los servicios del sistema no heredan ningún contexto (como las variables de entorno **HOME** y **PATH**) del usuario que los invoca y de su sesión. Cada servicio se ejecuta en un contexto de ejecución limpio.

- Cuando se carga un script de init de SysV, **systemd** lee la información de dependencia codificada en la cabecera Linux Standard Base (LSB) y la interpreta en tiempo de ejecución.

- Todas las operaciones en unidades de servicio están sujetas a un tiempo de espera por defecto de 5 minutos para evitar que un servicio que funcione mal congele el sistema. Este valor está codificado para los servicios que se generan a partir de los initscripts y no se puede cambiar. Sin embargo, se pueden utilizar archivos de configuración individuales para especificar un valor de tiempo de espera más largo por servicio, ver Ejemplo 3.11, "Cambiar el límite de tiempo de espera".

Para una lista detallada de los cambios de compatibilidad introducidos con **systemd**consulte el Manual de planificación de la migración para Red Hat Enterprise Linux 7.

3.2. GESTIÓN DE LOS SERVICIOS DEL SISTEMA

Las versiones anteriores de Red Hat Enterprise Linux, que se distribuían con SysV init o Upstart, utilizaban *init scripts* ubicado en el directorio **/etc/rc.d/init.d/**. Estos scripts de init estaban típicamente escritos en Bash y permitían al administrador del sistema controlar el estado de los servicios y demonios en su sistema. A partir de Red Hat Enterprise Linux 7, estos scripts de init han sido reemplazados por *service units*.

Las unidades de servicio terminan con la extensión de archivo **.service** y tienen un propósito similar al de los scripts de init. Para ver, iniciar, detener, reiniciar, habilitar o deshabilitar los servicios del sistema, utilice el comando **systemctl** como se describe en Comparación de la utilidad de servicio con systemctl , Comparación de la utilidad chkconfig con systemctl , y más adelante en esta sección. Los comandos **service** y **chkconfig** todavía están disponibles en el sistema y funcionan como se espera, pero sólo se incluyen por razones de compatibilidad y deben evitarse.

Tabla 3.3. Comparación de la utilidad de servicio con systemctl

servicio	systemctl	Descripción
service *name* start	**systemctl start *name*.service**	Inicia un servicio.
service *name* stop	**systemctl stop *name*.service**	Detiene un servicio.
service *name* restart	**systemctl restart *name*.service**	Reinicia un servicio.
service *name* condrestart	**systemctl try-restart *name*.service**	Reinicia un servicio sólo si se está ejecutando.
service *name* reload	**systemctl reload *name*.service**	Vuelve a cargar la configuración.
service *name* status	**systemctl status *name*.service** **systemctl is-active *name*.service**	Comprueba si un servicio se está ejecutando.
service --status-all	**systemctl list-units --type service --all**	Muestra el estado de todos los servicios.

Tabla 3.4. Comparación de la utilidad chkconfig con systemctl

chkconfig	systemctl	Descripción
chkconfig *name* on	**systemctl enable *name*.service**	Activa un servicio.
chkconfig *name* off	**systemctl disable *name*.service**	Desactiva un servicio.
chkconfig --list *name*	**systemctl status *name*.service** **systemctl is-enabled *name*.service**	Comprueba si un servicio está activado.
chkconfig --list	**systemctl list-unit-files --type service**	Enumera todos los servicios y comprueba si están activados.
chkconfig --list	**systemctl list-dependencies --after**	Enumera los servicios que se ordenan para comenzar antes de la unidad especificada.

chkconfig	systemctl	Descripción
chkconfig --list	**systemctl list-dependencies --before**	Enumera los servicios que se ordenan para iniciarse después de la unidad especificada.

Especificación de las unidades de servicio

Para mayor claridad, todos los ejemplos de comandos en el resto de esta sección utilizan nombres completos de unidades con la extensión de archivo **.service**, por ejemplo:

```
# systemctl stop nfs-server.service
```

Sin embargo, se puede omitir la extensión del archivo, en cuyo caso la utilidad **systemctl** asume que el argumento es una unidad de servicio. El siguiente comando es equivalente al anterior:

```
# systemctl stop nfs-server
```

Además, algunas unidades tienen nombres de alias. Esos nombres pueden tener nombres más cortos que las unidades, que pueden utilizarse en lugar de los nombres reales de las unidades. Para encontrar todos los alias que se pueden utilizar para una unidad en particular, utilice:

```
# systemctl show nfs-server.service -p Nombres
```

Comportamiento de systemctl en un entorno chroot

Si se cambia el directorio raíz utilizando el comando **chroot**, la mayoría de los comandos **systemctl** se niegan a realizar cualquier acción. La razón de esto es que el proceso **systemd** y el usuario que utilizó el comando **chroot** no tienen la misma vista del sistema de archivos. Esto sucede, por ejemplo, cuando se invoca **systemctl** desde un archivo **kickstart**.

La excepción a esto son los comandos de archivos de unidad como los comandos **systemctl enable** y **systemctl disable**. Estos comandos no necesitan un sistema en ejecución y no afectan a los procesos en ejecución, pero sí afectan a los archivos de unidad. Por lo tanto, puede ejecutar estos comandos incluso en el entorno **chroot**. Por ejemplo, para habilitar el servicio **httpd** en un sistema bajo el directorio **/srv/website1/**:

```
# chroot /srv/website1
# systemctl enable httpd.service
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service, pointing to
/usr/lib/systemd/system/httpd.service.
```

3.2.1. Servicios de listado

Para listar todas las unidades de servicio cargadas actualmente, escriba lo siguiente en un prompt del shell:

```
systemctl list-units --type service
```

Para cada archivo de unidad de servicio, este comando muestra su nombre completo (**UNIT**) seguido de una nota sobre si el archivo de unidad ha sido cargado (**LOAD**), su estado de activación de archivo de unidad de alto nivel (**ACTIVE**) y de bajo nivel (**SUB**), y una breve descripción (**DESCRIPTION**).

Por defecto, el comando **systemctl list-units** sólo muestra las unidades activas. Si desea listar todas las unidades cargadas independientemente de su estado, ejecute este comando con la opción de línea de comandos **--all** o **-a**:

```
systemctl list-units --type service --all
```

También puede listar todas las unidades de servicio disponibles para ver si están habilitadas. Para ello, escriba:

```
systemctl list-unit-files --type service
```

Para cada unidad de servicio, este comando muestra su nombre completo (**UNIT FILE**) seguido de información sobre si la unidad de servicio está habilitada o no (**STATE**). Para obtener información sobre cómo determinar el estado de las unidades de servicio individuales, consulte Visualización del estado del servicio.

Ejemplo 3.1. Servicios de listado

Para listar todas las unidades de servicio cargadas actualmente, ejecute el siguiente comando:

```
$ systemctl list-units --type service
UNIT                     LOAD   ACTIVE SUB     DESCRIPTION
abrt-ccpp.service        loaded active exited  Install ABRT coredump hook
abrt-oops.service        loaded active running ABRT kernel log watcher
abrt-vmcore.service      loaded active exited  Harvest vmcores for ABRT
abrt-xorg.service        loaded active running ABRT Xorg log watcher
abrtd.service            loaded active running ABRT Automated Bug Reporting Tool
…
systemd-vconsole-setup.service loaded active exited  Setup Virtual Console
tog-pegasus.service      loaded active running OpenPegasus CIM Server

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.

46 loaded units listed. Pass --all to see loaded but inactive units, too.
To show all installed unit files use 'systemctl list-unit-files'
```

Para listar todos los archivos de unidades de servicio instalados para determinar si están habilitados, escriba:

```
$ systemctl list-unit-files --type service
UNIT FILE                              STATE
abrt-ccpp.service                      enabled
abrt-oops.service                      enabled
abrt-vmcore.service                    enabled
abrt-xorg.service                      enabled
abrtd.service                          enabled
…
wpa_supplicant.service                 disabled
ypbind.service                         disabled

208 unit files listed.
```

3.2.2. Visualización del estado del servicio

Para mostrar información detallada sobre una unidad de servicio que corresponde a un servicio del sistema, escriba lo siguiente en un prompt del shell:

```
systemctl status name.service
```

Sustituya *name* por el nombre de la unidad de servicio que desea inspeccionar (por ejemplo, **gdm**). Este comando muestra el nombre de la unidad de servicio seleccionada seguido de su breve descripción, uno o más campos descritos en Tabla 3.5, "Información de la unidad de servicio disponible" , y si es ejecutado por el usuario **root**, también las entradas de registro más recientes.

Tabla 3.5. Información de la unidad de servicio disponible

Campo	Descripción
Loaded	Información sobre si se ha cargado la unidad de servicio, la ruta absoluta al archivo de la unidad y una nota sobre si la unidad está habilitada.
Active	Información sobre si la unidad de servicio está funcionando, seguida de una marca de tiempo.
Main PID	El PID del servicio del sistema correspondiente seguido de su nombre.
Status	Información adicional sobre el servicio del sistema correspondiente.
Process	Información adicional sobre los procesos relacionados.
CGroup	Información adicional sobre los grupos de control relacionados (cgroups).

Para verificar únicamente que una unidad de servicio en particular se está ejecutando, ejecute el siguiente comando:

```
systemctl is-active name.service
```

Del mismo modo, para determinar si una determinada unidad de servicio está habilitada, escriba:

```
systemctl is-enabled name.service
```

Tenga en cuenta que tanto **systemctl is-active** como **systemctl is-enabled** devuelven un estado de salida de **0** si la unidad de servicio especificada se está ejecutando o está habilitada. Para obtener información sobre cómo listar todas las unidades de servicio cargadas actualmente, consulte Listado de servicios.

Ejemplo 3.2. Visualización del estado del servicio

La unidad de servicio para el gestor de pantalla de GNOME se llama **gdm.service**. Para determinar el estado actual de esta unidad de servicio, escriba lo siguiente en un prompt del shell:

```
# systemctl status gdm.service
gdm.service - GNOME Display Manager
   Loaded: loaded (/usr/lib/systemd/system/gdm.service; enabled)
   Active: active (running) since Thu 2013-10-17 17:31:23 CEST; 5min ago
 Main PID: 1029 (gdm)
   CGroup: /system.slice/gdm.service
           ├─1029 /usr/sbin/gdm
           ├─1037 /usr/libexec/gdm-simple-slave --display-id /org/gno…
           └─1047 /usr/bin/Xorg :0 -background none -verbose -auth /r…

Oct 17 17:31:23 localhost systemd[1]: Started GNOME Display Manager.
```

Ejemplo 3.3. Visualización de los servicios ordenados a iniciar antes de un servicio

Para determinar qué servicios se ordenan para iniciarse antes que el servicio especificado, escriba lo siguiente en un prompt del shell:

```
# systemctl list-dependencies --after gdm.service
gdm.service
├─dbus.socket
├─getty@tty1.service
├─livesys.service
├─plymouth-quit.service
├─system.slice
├─systemd-journald.socket
├─systemd-user-sessions.service
└─basic.target
[output truncated]
```

Ejemplo 3.4. Visualización de los servicios ordenados a iniciar después de un servicio

Para determinar qué servicios se ordenan para iniciarse después del servicio especificado, escriba lo siguiente en un prompt del shell:

```
# systemctl list-dependencies --before gdm.service
gdm.service
├─dracut-shutdown.service
├─graphical.target
│ ├─systemd-readahead-done.service
│ ├─systemd-readahead-done.timer
│ └─systemd-update-utmp-runlevel.service
└─shutdown.target
  ├─systemd-reboot.service
  └─final.target
    └─systemd-reboot.service
```

3.2.3. Iniciar un servicio

Para iniciar una unidad de servicio que corresponde a un servicio del sistema, escriba lo siguiente en un indicador del shell como **root**:

systemctl start *name*.service

Sustituya *name* por el nombre de la unidad de servicio que desea iniciar (por ejemplo, **gdm**). Este comando inicia la unidad de servicio seleccionada en la sesión actual. Para obtener información sobre cómo activar una unidad de servicio para que se inicie en el momento del arranque, consulte Activación de un servicio. Para obtener información sobre cómo determinar el estado de una determinada unidad de servicio, consulte Visualización del estado del servicio.

Ejemplo 3.5. Iniciar un servicio

La unidad de servicio para el servidor HTTP Apache se llama **httpd.service**. Para activar esta unidad de servicio e iniciar el demonio **httpd** en la sesión actual, ejecute el siguiente comando como **root**:

```
# systemctl start httpd.service
```

3.2.4. Detener un servicio

Para detener una unidad de servicio que corresponde a un servicio del sistema, escriba lo siguiente en un indicador del shell como **root**:

systemctl stop *name*.service

Sustituya *name* por el nombre de la unidad de servicio que desea detener (por ejemplo, **bluetooth**). Este comando detiene la unidad de servicio seleccionada en la sesión actual. Para obtener información sobre cómo desactivar una unidad de servicio y evitar que se inicie en el momento del arranque, consulte Desactivación de un servicio. Para obtener información sobre cómo determinar el estado de una determinada unidad de servicio, consulte Visualización del estado del servicio.

Ejemplo 3.6. Detener un servicio

La unidad de servicio para el demonio **bluetoothd** se llama **bluetooth.service**. Para desactivar esta unidad de servicio y detener el demonio **bluetoothd** en la sesión actual, ejecute el siguiente comando como **root**:

```
# systemctl stop bluetooth.service
```

3.2.5. Reiniciar un servicio

Para reiniciar una unidad de servicio que corresponde a un servicio del sistema, escriba lo siguiente en un indicador del shell como **root**:

systemctl restart *name*.service

Sustituya *name* por el nombre de la unidad de servicio que desea reiniciar (por ejemplo, **httpd**). Este comando detiene la unidad de servicio seleccionada en la sesión actual y la reinicia inmediatamente. Es importante destacar que si la unidad de servicio seleccionada no está en funcionamiento, este comando

también la inicia. Para indicar **systemd** que reinicie una unidad de servicio sólo si el servicio correspondiente ya se está ejecutando, ejecute el siguiente comando como **root**:

```
systemctl try-restart name.service
```

Algunos servicios del sistema también permiten recargar su configuración sin interrumpir su ejecución. Para ello, escriba como **root**:

```
systemctl reload name.service
```

Tenga en cuenta que los servicios del sistema que no soportan esta función ignoran este comando por completo. Por comodidad, el comando **systemctl** también admite los comandos **reload-or-restart** y **reload-or-try-restart** que reinician dichos servicios en su lugar. Para obtener información sobre cómo determinar el estado de una determinada unidad de servicio, consulte Visualización del estado del servicio.

Ejemplo 3.7. Reiniciar un servicio

Para evitar que los usuarios se encuentren con mensajes de error innecesarios o con páginas web parcialmente renderizadas, el servidor HTTP Apache permite editar y recargar su configuración sin necesidad de reiniciarlo e interrumpir las peticiones procesadas activamente. Para ello, escriba lo siguiente en un prompt del shell como **root**:

```
# systemctl reload httpd.service
```

3.2.6. Habilitar un servicio

Para configurar una unidad de servicio que corresponda a un servicio del sistema para que se inicie automáticamente en el momento del arranque, escriba lo siguiente en un indicador del shell como **root**:

```
systemctl enable name.service
```

Sustituya *name* por el nombre de la unidad de servicio que desea activar (por ejemplo, **httpd**). Este comando lee la sección **[Install]** de la unidad de servicio seleccionada y crea los enlaces simbólicos apropiados al archivo **/usr/lib/systemd/system/*name*.service** en el directorio **/etc/systemd/system/** y sus subdirectorios. Sin embargo, este comando no reescribe los enlaces que ya existen. Si quiere asegurarse de que los enlaces simbólicos se vuelven a crear, utilice el siguiente comando como **root**:

```
systemctl reenable name.service
```

Este comando desactiva la unidad de servicio seleccionada y la vuelve a activar inmediatamente. Para obtener información sobre cómo determinar si una determinada unidad de servicio está habilitada para iniciarse en el momento del arranque, consulte Visualización del estado del servicio . Para obtener información sobre cómo iniciar un servicio en la sesión actual, consulte Iniciar un servicio.

Ejemplo 3.8. Habilitar un servicio

Para configurar el servidor HTTP Apache para que se inicie automáticamente en el momento del arranque, ejecute el siguiente comando como **root**:

```
# systemctl enable httpd.service
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to
/usr/lib/systemd/system/httpd.service.
```

3.2.7. Desactivar un servicio

Para evitar que una unidad de servicio que corresponde a un servicio del sistema se inicie automáticamente en el momento del arranque, escriba lo siguiente en un indicador del shell como **root**:

systemctl disable *name*.service

Sustituya *name* por el nombre de la unidad de servicio que desea desactivar (por ejemplo, **bluetooth**). Este comando lee la sección **[Install]** de la unidad de servicio seleccionada y elimina los enlaces simbólicos apropiados al archivo **/usr/lib/systemd/system/*name*.service** del directorio **/etc/systemd/system/** y sus subdirectorios. Además, puedes enmascarar cualquier unidad de servicio para evitar que sea iniciada manualmente o por otro servicio. Para ello, ejecute el siguiente comando como **root**:

systemctl mask *name*.service

Este comando sustituye el archivo **/etc/systemd/system/*name*.service** con un enlace simbólico a **/dev/null**, haciendo que el archivo de la unidad real sea inaccesible para **systemd**. Para revertir esta acción y desenmascarar una unidad de servicio, escriba como **root**:

systemctl unmask *name*.service

Para obtener información sobre cómo determinar si una determinada unidad de servicio está habilitada para iniciarse en el momento del arranque, consulte Visualización del estado del servicio . Para obtener información sobre cómo detener un servicio en la sesión actual, consulte Detener un servicio.

Ejemplo 3.9. Desactivar un servicio

Ejemplo 3.6, “Detener un servicio” ilustra cómo detener la unidad **bluetooth.service** en la sesión actual. Para evitar que esta unidad de servicio se inicie en el momento del arranque, escriba lo siguiente en un indicador del shell como **root**:

```
# systemctl disable bluetooth.service
Removed symlink /etc/systemd/system/bluetooth.target.wants/bluetooth.service.
Removed symlink /etc/systemd/system/dbus-org.bluez.service.
```

3.2.8. Iniciar un servicio conflictivo

En **systemd**existen dependencias positivas y negativas entre los servicios. El inicio de un servicio particular puede requerir el inicio de uno o más servicios (dependencia positiva) o la detención de uno o más servicios (dependencia negativa).

Cuando se intenta iniciar un nuevo servicio **systemd** resuelve todas las dependencias automáticamente. Tenga en cuenta que esto se hace sin notificación explícita al usuario. Si ya se está ejecutando un servicio, y se intenta iniciar otro servicio con una dependencia negativa, el primer servicio se detiene automáticamente.

Por ejemplo, si está ejecutando el servicio **postfix**, y trata de iniciar el servicio **sendmail**, **systemd** primero detiene automáticamente **postfix**, porque estos dos servicios entran en conflicto y no pueden ejecutarse en el mismo puerto.

3.3. TRABAJAR CON OBJETIVOS SYSTEMD

Los objetivos de systemd están representados por unidades de objetivo. Los archivos de las unidades objetivo terminan con la extensión de archivo **.target** y su único propósito es agrupar otras unidades systemd a través de una cadena de dependencias. Por ejemplo, la unidad **graphical.target unit**, que se utiliza para iniciar una sesión gráfica, inicia servicios del sistema como el gestor de pantalla de GNOME **(gdm.service)** o el servicio de cuentas **(accounts-daemon.service)** y también activa la unidad **multi-user.target unit**. De manera similar, la unidad multiusuario.target inicia otros servicios esenciales del sistema como NetworkManager **(NetworkManager.service)** o D-Bus **(dbus.service)** y activa otra unidad target llamada basic.target.

Esta sección incluye los procedimientos que deben aplicarse cuando se trabaja con los objetivos de **systemd**.

3.3.1. Diferencia entre los niveles de ejecución de SysV y los objetivos de systemd

Las versiones anteriores de Red Hat Enterprise Linux se distribuían con SysV init o Upstart, e implementaban un conjunto predefinido de niveles de ejecución que representaban modos específicos de operación. Estos niveles de ejecución estaban numerados del 0 al 6 y eran definidos por una selección de servicios del sistema que se ejecutaban cuando un nivel de ejecución particular era habilitado por el administrador del sistema. A partir de Red Hat Enterprise Linux 7, el concepto de niveles de ejecución ha sido reemplazado por los objetivos de systemd.

Red Hat Enterprise Linux 7 fue distribuido con un número de objetivos predefinidos que son más o menos similares al conjunto estándar de niveles de ejecución de las versiones anteriores. Por razones de compatibilidad, también proporciona alias para estos objetivos que se asignan directamente a los niveles de ejecución SysV.

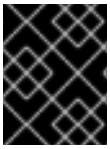
La siguiente tabla proporciona una lista completa de los niveles de ejecución de SysV y sus correspondientes objetivos de systemd:

Tabla 3.6. Comparación de los niveles de ejecución de SysV con los objetivos de systemd

Runlevel	Unidades de destino	Descripción
0	**runlevel0.target**, **poweroff.target**	Apague y desconecte el sistema.
1	**runlevel1.target**, **rescue.target**	Prepara un caparazón de rescate.
2	**runlevel2.target**, **multi-user.target**	Configurar un sistema multiusuario no gráfico.
3	**runlevel3.target**, **multi-user.target**	Configurar un sistema multiusuario no gráfico.
4	**runlevel4.target**, **multi-user.target**	Configurar un sistema multiusuario no gráfico.

Runlevel	Unidades de destino	Descripción
5	**runlevel5.target**, **graphical.target**	Configurar un sistema gráfico multiusuario.
6	**runlevel6.target**, **reboot.target**	Apague y reinicie el sistema.

La siguiente tabla compara los comandos SysV init con systemctl. Utilice la utilidad systemctl para ver, cambiar o configurar los objetivos de systemd:



IMPORTANTE

Los comandos **runlevel** y **telinit** todavía están disponibles en el sistema y funcionan como se espera, pero sólo se incluyen por razones de compatibilidad y deben evitarse.

Tabla 3.7. Comparación de los comandos SysV init con systemctl

Antiguo Mando	Nuevo mando	Descripción
runlevel	**systemctl list-units --type target**	Enumera las unidades objetivo cargadas actualmente.
telinit *runlevel*	**systemctl isolate *name*.target**	Cambia el objetivo actual.

Recursos adicionales

- man sysv init
- man upstart init
- man systemctl

3.3.2. Ver el objetivo por defecto

La unidad de destino por defecto está representada por el archivo **/etc/systemd/system/default.target**.

Procedimiento

- Para determinar qué unidad de destino se utiliza por defecto:

```
$ systemctl get-default
graphical.target
```

- Para determinar el objetivo por defecto utilizando el enlace simbólico:

```
$  ls -l /lib/systemd/system/default.target
```

3.3.3. Visualización de las unidades de destino

Por defecto, el comando **systemctl list-units** sólo muestra las unidades activas.

Procedimiento

- Para listar todas las unidades cargadas independientemente de su estado:

```
$ systemctl list-units --type target --all
```

- Para listar todas las unidades de destino cargadas actualmente:

```
$ systemctl list-units --type target

UNIT                   LOAD   ACTIVE SUB    DESCRIPTION
basic.target           loaded active active Basic System
cryptsetup.target      loaded active active Encrypted Volumes
getty.target           loaded active active Login Prompts
graphical.target       loaded active active Graphical Interface
local-fs-pre.target    loaded active active Local File Systems (Pre)
local-fs.target        loaded active active Local File Systems
multi-user.target      loaded active active Multi-User System
network.target         loaded active active Network
paths.target           loaded active active Paths
remote-fs.target       loaded active active Remote File Systems
sockets.target         loaded active active Sockets
sound.target           loaded active active Sound Card
spice-vdagentd.target loaded active active Agent daemon for Spice guests
swap.target            loaded active active Swap
sysinit.target         loaded active active System Initialization
time-sync.target       loaded active active System Time Synchronized
timers.target          loaded active active Timers

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.

17 loaded units listed.
```

3.3.4. Cambiar el objetivo por defecto

La unidad de destino por defecto está representada por el archivo **/etc/systemd/system/default.target**. El siguiente procedimiento describe cómo cambiar el objetivo por defecto utilizando el comando systemctl:

Procedimiento

1. Para determinar la unidad de destino por defecto:

```
# systemctl get-default
```

2. Para configurar el sistema para utilizar una unidad de destino diferente por defecto:

```
# systemctl set-default multi-user.target
rm /etc/systemd/system/default.target
ln -s /usr/lib/systemd/system/multi-user.target /etc/systemd/system/default.target
```

Este comando reemplaza el archivo **/etc/systemd/system/default.target** con un enlace simbólico a **/usr/lib/systemd/system/name.target**, donde nombre es el nombre de la unidad de destino que desea utilizar. Sustituya *multi-user* por el nombre de la unidad de destino que desee utilizar por defecto.

3. Reiniciar

```
# rebote
```

3.3.5. Cambio de destino por defecto mediante enlace simbólico

El siguiente procedimiento describe cómo cambiar el destino por defecto creando un enlace simbólico al mismo.

Procedimiento

1. Para determinar la unidad de destino por defecto:

```
#  ls /lib/systemd/system/default.target -l
```

2. Para crear un enlace simbólico:

```
#  ln -sf /lib/systemd/system/graphical.target /etc/systemd/system/default.target
```

3. Reinicie el sistema:

```
# rebote
```

Pasos de verificación

- Verifica el nuevo default.target creado:

```
$ systemctl get-default
multi-user.target
```

3.3.6. Cambiar el objetivo actual

Este procedimiento explica cómo cambiar la unidad de destino en la sesión actual utilizando el comando systemctl.

Procedimiento

- Para cambiar a una unidad de destino diferente en la sesión actual:

```
# systemctl isolate multi-user.target
```

Este comando inicia la unidad de destino llamada *multi-user* y todas las unidades dependientes, y detiene inmediatamente todas las demás.

Sustituya *multi-user* por el nombre de la unidad de destino que desee utilizar por defecto.

Pasos de verificación

- Verifica el nuevo default.target creado:

```
$ systemctl get-default
multi-user.target
```

3.3.7. Arranque en modo de rescate

Rescue mode proporciona un cómodo entorno de usuario único y permite reparar el sistema en situaciones en las que no puede completar un proceso de arranque normal. En el modo de rescate, el sistema intenta montar todos los sistemas de archivos locales e iniciar algunos servicios importantes del sistema, pero no activa las interfaces de red ni permite que haya más usuarios conectados al sistema al mismo tiempo.

Procedimiento

- Para cambiar el objetivo actual y entrar en el modo de rescate en la sesión actual:

```
# systemctl rescue

Broadcast message from root@localhost on pts/0 (Fri 2013-10-25 18:23:15 CEST):

The system is going down to rescue mode NOW!
```

  Este comando es similar a **systemctl isolate rescue.target**, pero también envía un mensaje informativo a todos los usuarios que están actualmente conectados al sistema.

  Para evitar que **systemd** envíe un mensaje, ejecute el siguiente comando con la opción de línea de comandos **--no-wall # systemctl --no-wall rescue**

3.3.8. Arranque en modo de emergencia

Emergency mode proporciona el entorno más mínimo posible y permite reparar el sistema incluso en situaciones en las que el sistema no puede entrar en modo de rescate. En el modo de emergencia, el sistema monta el sistema de archivos raíz sólo para lectura, no intenta montar ningún otro sistema de archivos local, no activa las interfaces de red y sólo inicia unos pocos servicios esenciales.

Procedimiento

- Para cambiar el objetivo actual y entrar en el modo de emergencia:

```
# systemctl emergency
```

Este comando es similar a **systemctl isolate emergency.target**, pero también envía un mensaje informativo a todos los usuarios que están actualmente conectados al sistema.

Para evitar que systemd envíe este mensaje, ejecute el siguiente comando con la opción de línea de comandos **--no-wall # systemctl --no-wall emergency**

3.4. APAGAR, SUSPENDER E HIBERNAR EL SISTEMA

En Red Hat Enterprise Linux 7, la utilidad **systemctl** reemplazó varios comandos de gestión de energía utilizados en versiones anteriores de Red Hat Enterprise Linux. Los comandos listados en Tabla 3.8, "Comparación de los comandos de gestión de energía con systemctl" todavía están disponibles en el sistema por razones de compatibilidad, pero se aconseja que utilice **systemctl** cuando sea posible.

Tabla 3.8. Comparación de los comandos de gestión de energía con systemctl

Antiguo Mando	Nuevo mando	Descripción
halt	**systemctl halt**	Detiene el sistema.
poweroff	**systemctl poweroff**	Apaga el sistema.
reboot	**systemctl reboot**	Reinicia el sistema.
pm-suspend	**systemctl suspend**	Suspende el sistema.
pm-hibernate	**systemctl hibernate**	Hiberna el sistema.
pm-suspend-hybrid	**systemctl hybrid-sleep**	Hiberna y suspende el sistema.

3.4.1. Apagar el sistema

La utilidad **systemctl** proporciona comandos para apagar el sistema, sin embargo el comando tradicional **shutdown** también es soportado. Aunque el comando **shutdown** llamará a la utilidad **systemctl** para realizar el apagado, tiene la ventaja de que también admite un argumento de tiempo. Esto es particularmente útil para el mantenimiento programado y para dar más tiempo a los usuarios para reaccionar al aviso de que se ha programado un cierre del sistema. La opción de cancelar el apagado también puede ser una ventaja.

Uso de los comandos systemctl

Para apagar el sistema y desconectar la máquina, escriba lo siguiente en un prompt del shell como **root**:

```
systemctl poweroff
```

Para apagar y detener el sistema sin apagar la máquina, ejecute el siguiente comando como **root**:

```
systemctl halt
```

Por defecto, la ejecución de cualquiera de estos comandos hace que **systemd** envíe un mensaje informativo a todos los usuarios que estén conectados al sistema. Para evitar **systemd** el envío de este mensaje, ejecute el comando seleccionado con la opción de línea de comandos **--no-wall**, por ejemplo:

```
systemctl --no-wall poweroff
```

Utilizar el comando de apagado

Para apagar el sistema y desconectar la máquina a una hora determinada, utilice un comando con el siguiente formato como **root**:

```
shutdown --poweroff hh:mm
```

Donde *hh:mm* es la hora en formato de reloj de 24 horas. El archivo **/run/nologin** se crea 5 minutos antes de que se apague el sistema para evitar nuevos inicios de sesión. Cuando se utiliza un argumento de tiempo, se puede añadir al comando un mensaje opcional, el *wall message*.

Para apagar y detener el sistema después de un retraso, sin apagar la máquina, utilice un comando con el siguiente formato como **root**:

```
apagado --halt m
```

Donde *m* es el tiempo de retraso en minutos. La palabra clave **now** es un alias de **0**.

El usuario de **root** puede cancelar un cierre pendiente de la siguiente manera:

```
shutdown -c
```

Consulte la página del manual **shutdown(8)** para conocer otras opciones de comandos.

3.4.2. Reiniciar el sistema

Para reiniciar el sistema, ejecute el siguiente comando como **root**:

```
systemctl reboot
```

Por defecto, este comando hace que **systemd** envíe un mensaje informativo a todos los usuarios que están actualmente conectados al sistema. Para evitar **systemd** el envío de este mensaje, ejecute este comando con la opción de línea de comandos **--no-wall**:

```
systemctl --no-wall reboot
```

3.4.3. Suspender el sistema

Para suspender el sistema, escriba lo siguiente en un prompt del shell como **root**:

```
systemctl suspend
```

Este comando guarda el estado del sistema en la RAM y, con la excepción del módulo RAM, apaga la mayoría de los dispositivos de la máquina. Cuando se vuelve a encender la máquina, el sistema restaura su estado desde la RAM sin tener que arrancar de nuevo. Como el estado del sistema se guarda en la RAM y no en el disco duro, restaurar el sistema desde el modo de suspensión es significativamente más rápido que restaurarlo desde la hibernación, pero como consecuencia, un estado de sistema suspendido también es vulnerable a los cortes de energía.

Para obtener información sobre cómo hibernar el sistema, consulte Sección 3.4.4, “Hibernación del sistema”.

3.4.4. Hibernación del sistema

Para hibernar el sistema, escriba lo siguiente en un indicador del shell como **root**:

```
systemctl hibernate
```

Este comando guarda el estado del sistema en el disco duro y apaga la máquina. Cuando se vuelve a

encender la máquina, el sistema restaura su estado a partir de los datos guardados sin tener que arrancar de nuevo. Como el estado del sistema se guarda en el disco duro y no en la RAM, la máquina no tiene que mantener la energía eléctrica en el módulo de RAM, pero como consecuencia, restaurar el sistema desde la hibernación es significativamente más lento que restaurarlo desde el modo de suspensión.

Para hibernar y suspender el sistema, ejecute el siguiente comando como **root**:

```
systemctl hybrid-sleep
```

Para obtener información sobre cómo suspender el sistema, consulte Sección 3.4.3, "Suspender el sistema".

3.5. TRABAJAR CON ARCHIVOS DE UNIDAD SYSTEMD

Este capítulo incluye la descripción de los archivos de unidad de systemd. Las siguientes secciones le muestran cómo:

- Crear archivos de unidad personalizados
- Convertir los scripts de init de SysV en archivos unitarios
- Modificar los archivos de las unidades existentes
- Trabajar con unidades instanciadas

3.5.1. Introducción a los archivos de la unidad

Un archivo de unidad contiene directivas de configuración que describen la unidad y definen su comportamiento. Varios comandos de **systemctl** trabajan con archivos de unidad en segundo plano. Para realizar ajustes más finos, el administrador del sistema debe editar o crear archivos de unidad manualmente. Tabla 3.1, "Ubicación de los archivos de la unidad Systemd" enumera tres directorios principales donde se almacenan los archivos de unidad en el sistema, el directorio **/etc/systemd/system/** está reservado para los archivos de unidad creados o personalizados por el administrador del sistema.

Los nombres de los archivos de las unidades tienen la siguiente forma:

```
unit_nametype_extension
```

Aquí, *unit_name* representa el nombre de la unidad y *type_extension* identifica el tipo de unidad, véase Tabla 3.2, "Tipos de unidades systemd disponibles" para una lista completa de tipos de unidad. Por ejemplo, normalmente hay **sshd.service** así como **sshd.socket** unidad presente en su sistema.

Los archivos de unidad pueden complementarse con un directorio para archivos de configuración adicionales. Por ejemplo, para añadir opciones de configuración personalizadas a **sshd.service**, cree el archivo **sshd.service.d/custom.conf** e inserte allí las directivas adicionales. Para obtener más información sobre los directorios de configuración, consulte Modificación de los archivos de unidad existentes.

También se pueden crear los directorios **sshd.service.wants/** y **sshd.service.requires/**. Estos directorios contienen enlaces simbólicos a archivos de unidad que son dependencias del servicio **sshd**. Los enlaces simbólicos se crean automáticamente durante la instalación según las opciones de archivos

de unidad [Install] o en tiempo de ejecución según las opciones [Unit]. También es posible crear estos directorios y enlaces simbólicos manualmente. Para más detalles sobre las opciones [Install] y [Unit], consulte las tablas siguientes.

Muchas de las opciones de los archivos de unidad pueden establecerse mediante las denominadas **unit specifiers**, cadenas comodín que se sustituyen dinámicamente por parámetros de unidad cuando se carga el archivo de unidad. Esto permite la creación de archivos de unidad genéricos que sirven como plantillas para generar unidades instanciadas. Para más detalles, véase Trabajar con unidades instanciadas.

3.5.2. Estructura del archivo de la unidad

Los archivos unitarios suelen constar de tres secciones:

- La sección **[Unit]** - contiene opciones genéricas que no dependen del tipo de unidad. Estas opciones proporcionan la descripción de la unidad, especifican el comportamiento de la unidad y establecen dependencias con otras unidades. Para ver una lista de las opciones [Unit] más utilizadas, consulte Tabla 3.9, "Opciones importantes de la sección [Unidad]" .
- La sección **[Unit type]** - si una unidad tiene directivas específicas de tipo, éstas se agrupan en una sección que lleva el nombre del tipo de unidad. Por ejemplo, los archivos de unidades de servicio contienen la sección **[Service]**.
- La sección **[Install]** - contiene información sobre la instalación de unidades utilizada por los comandos **systemctl enable** y **disable**. Para obtener una lista de opciones de la sección **[Install]**, consulte Tabla 3.11, "Opciones importantes de la sección [Instalar]" .

3.5.2.1. Opciones importantes de la sección [Unidad]

Las siguientes tablas enumeran las opciones importantes de la sección [Unidad].

Tabla 3.9. Opciones importantes de la sección [Unidad]

Opción[a]	Descripción
Description	Una descripción significativa de la unidad. Este texto se muestra, por ejemplo, en la salida del comando **systemctl status**.
Documentation	Proporciona una lista de URIs que hacen referencia a la documentación de la unidad.
After[b]	Define el orden de inicio de las unidades. La unidad se inicia sólo después de que las unidades especificadas en **After** estén activas. A diferencia de **Requires**, **After** no activa explícitamente las unidades especificadas. La opción **Before** tiene la funcionalidad opuesta a **After**.
Requires	Configura las dependencias de otras unidades. Las unidades listadas en **Requires** se activan junto con la unidad. Si alguna de las unidades requeridas no se inicia, la unidad no se activa.

Opción[a]	Descripción
Wants	Configura dependencias más débiles que **Requires**. Si alguna de las unidades listadas no se inicia con éxito, no tiene impacto en la activación de la unidad. Esta es la forma recomendada para establecer dependencias de unidades personalizadas.
Conflicts	Configura las dependencias negativas, un opuesto a **Requires**.

[a] Para obtener una lista completa de las opciones configurables en la sección [Unidad], consulte la página del manual **systemd.unit(5)**.

[b] En la mayoría de los casos, basta con establecer sólo las relaciones de ordenación con las opciones de archivo de unidad **After** y **Before**. Si también se establece una dependencia de requisitos con **Wants** (recomendado) o **Requires**, la dependencia de ordenación aún debe ser especificada. Esto se debe a que las dependencias de ordenación y de requisitos funcionan de forma independiente.

3.5.2.2. Opciones importantes de la sección [Servicio]

Las siguientes tablas enumeran las opciones importantes de la sección [Servicio].

Tabla 3.10. Opciones importantes de la sección [Servicio]

Opción[a]	Descripción

Opción[a]	Descripción
Type	Configura el tipo de inicio del proceso de la unidad que afecta a la funcionalidad de **ExecStart** y las opciones relacionadas. Uno de: * **simple** - El valor por defecto. El proceso iniciado con **ExecStart** es el proceso principal del servicio. * **forking** - El proceso iniciado con**ExecStart** genera un proceso hijo que se convierte en el proceso principal del servicio. El proceso principal sale cuando se completa el inicio. * **oneshot** - Este tipo es similar a**simple**, pero el proceso sale antes de iniciar las unidades consecuentes. * **dbus** - Este tipo es similar a**simple**, pero las unidades consecuentes se inician sólo después de que el proceso principal obtenga un nombre D-Bus. * **notify** - Este tipo es similar a**simple**, pero las unidades consecuentes se inician sólo después de que se envíe un mensaje de notificación a través de la función sd_notify(). * **idle** - similar a**simple**, la ejecución real del binario del servicio se retrasa hasta que todos los trabajos hayan terminado, lo que evita mezclar la salida de estado con la salida del shell de los servicios.
ExecStart	Especifica los comandos o scripts que se ejecutarán cuando se inicie la unidad. **ExecStartPre** y **ExecStartPost** especifican los comandos personalizados que se ejecutarán antes y después de **ExecStart**. **Type=oneshot** permite especificar varios comandos personalizados que se ejecutan secuencialmente.
ExecStop	Especifica los comandos o scripts que se ejecutarán cuando la unidad se detenga.
ExecReload	Especifica los comandos o scripts que se ejecutarán cuando se recargue la unidad.
Restart	Con esta opción activada, el servicio se reinicia tras la salida de su proceso, a excepción de una parada limpia mediante el comando **systemctl**.

Opción[a]	Descripción
RemainAfterExit	Si se establece como True, el servicio se considera activo incluso cuando todos sus procesos han salido. El valor por defecto es Falso. Esta opción es especialmente útil si se configura **Type=oneshot**.

[a] Para obtener una lista completa de las opciones configurables en la sección [Servicio], consulte la página del manual **systemd.service(5)**.

3.5.2.3. Opciones importantes de la sección [Instalar]

Las siguientes tablas enumeran las opciones importantes de la sección [Instalar].

Tabla 3.11. Opciones importantes de la sección [Instalar]

Opción[a]	Descripción
Alias	Proporciona una lista separada por espacios de nombres adicionales para la unidad. La mayoría de los comandos de **systemctl**, excepto **systemctl enable**, pueden utilizar alias en lugar del nombre real de la unidad.
RequiredBy	Una lista de unidades que dependen de la unidad. Cuando se habilita esta unidad, las unidades enumeradas en **RequiredBy** adquieren una dependencia de la unidad **Require**.
WantedBy	Una lista de unidades que dependen débilmente de la unidad. Cuando se habilita esta unidad, las unidades listadas en **WantedBy** ganan una dependencia de la unidad **Want**.
Also	Especifica una lista de unidades a instalar o desinstalar junto con la unidad.
DefaultInstance	Limitada a las unidades instanciadas, esta opción especifica la instancia por defecto para la que se habilita la unidad. Véase Trabajar conunidades instanciadas

[a] Para obtener una lista completa de las opciones configurables en la sección [Instalar], consulte la página del manual **systemd.unit(5)**.

3.5.3. Creación de archivos de unidad personalizados

Hay varios casos de uso para crear archivos de unidad desde cero: podría ejecutar un demonio personalizado, crear una segunda instancia de algún servicio existente (como en Crear una segunda

instancia del servicio sshd), o importar un script de init de SysV (más en Convertir scripts de init de SysV en archivos de unidad). Por otro lado, si sólo pretende modificar o ampliar el comportamiento de una unidad existente, utilice las instrucciones de Modificar archivos de unidad existentes. El siguiente procedimiento describe el proceso general de creación de un servicio personalizado.

Procedimiento

1. Prepare el archivo ejecutable con el servicio personalizado. Puede ser un script creado a medida o un ejecutable entregado por un proveedor de software. Si es necesario, prepara un archivo PID para mantener un PID constante para el proceso principal del servicio personalizado. También es posible incluir archivos de entorno para almacenar variables de shell para el servicio. Asegúrese de que el script fuente es ejecutable (ejecutando el **chmod a x**) y no es interactivo.

2. Cree un archivo de unidad en el directorio **/etc/systemd/system/** y asegúrese de que tiene los permisos correctos. Ejecute como **root**:

   ```
   touch /etc/systemd/system/name.service

   chmod 664 /etc/systemd/system/name.service
   ```

   Sustituya *name* por el nombre del servicio a crear. Tenga en cuenta que no es necesario que el archivo sea ejecutable.

3. Abra el archivo ***name*.service** creado en el paso anterior y añada las opciones de configuración del servicio. Hay una variedad de opciones que se pueden utilizar dependiendo del tipo de servicio que se desea crear, ver Estructura del archivo de la unidad. El siguiente es un ejemplo de configuración de unidad para un servicio relacionado con la red:

   ```
   [Unit]
   Description=service_description
   After=network.target

   [Service]
   ExecStart=path_to_executable
   Type=forking
   PIDFile=path_to_pidfile

   [Install]
   WantedBy=default.target
   ```

   Dónde:

   - *service_description* es una descripción informativa que se muestra en los archivos de registro del diario y en la salida del comando **systemctl status**.
   - el ajuste **After** garantiza que el servicio se inicie sólo después de que la red esté en funcionamiento. Añade una lista separada por espacios de otros servicios u objetivos relevantes.
   - *path_to_executable* representa la ruta del ejecutable del servicio real.
   - **Type=forking** se utiliza para los demonios que hacen la llamada al sistema fork. El proceso principal del servicio se crea con el PID especificado en *path_to_pidfile*. Encuentra otros tipos de inicio en Tabla 3.10, “Opciones importantes de la sección [Servicio]” .

- **WantedBy** establece el objetivo o los objetivos con los que debe iniciarse el servicio. Piensa en estos objetivos como un reemplazo del antiguo concepto de niveles de ejecución.

4. Notificar a **systemd** que existe un nuevo ***name*.service** archivo existe ejecutando el siguiente comando como **root**:

```
systemctl daemon-reload

systemctl start name.service
```

AVISO

Ejecute siempre el comando **systemctl daemon-reload** después de crear nuevos archivos de unidad o de modificar los existentes. De lo contrario, los comandos **systemctl start** o **systemctl enable** podrían fallar debido a un desajuste entre los estados de **systemd** y los archivos de unidad de servicio reales en el disco. Tenga en cuenta que en sistemas con un gran número de unidades esto puede llevar mucho tiempo, ya que el estado de cada unidad tiene que ser serializado y posteriormente deserializado durante la recarga.

3.5.3.1. Creación de un archivo de unidad personalizado utilizando la segunda instancia del servicio sshd

Los administradores de sistemas a menudo necesitan configurar y ejecutar múltiples instancias de un servicio. Esto se hace creando copias de los archivos de configuración del servicio original y modificando ciertos parámetros para evitar conflictos con la instancia primaria del servicio. El siguiente procedimiento muestra cómo crear una segunda instancia del servicio **sshd**.

Procedimiento

1. Cree una copia del archivo **sshd_config** que será utilizado por el segundo demonio:

```
# cp /etc/ssh/sshd{,-segundo}_config
```

2. Edite el archivo **sshd-second_config** creado en el paso anterior para asignar un número de puerto y un archivo PID diferentes al segundo demonio:

```
Port 22220
PidFile /var/run/sshd-second.pid
```

   Consulte la página del manual **sshd_config**(5) para obtener más información sobre las opciones **Port** y **PidFile**. Asegúrese de que el puerto elegido no está siendo utilizado por ningún otro servicio. El archivo PID no tiene que existir antes de ejecutar el servicio, se genera automáticamente al iniciar el servicio.

3. Cree una copia del archivo de unidad systemd para el servicio **sshd**:

```
# cp /usr/lib/systemd/system/sshd.service /etc/systemd/system/sshd-second.service
```

4. Altere el **sshd-second.service** creado en el paso anterior como sigue:

   a. Modificar la opción **Description**:

   ```
   Descripción=Demonio de segunda instancia del servidor OpenSSH
   ```

   b. Añade sshd.service a los servicios especificados en la opción **After**, para que la segunda instancia se inicie sólo después de que la primera ya se haya iniciado:

   ```
   After=syslog.target network.target auditd.service sshd.service
   ```

   c. La primera instancia de sshd incluye la generación de claves, por lo tanto, elimine la línea **ExecStartPre=/usr/sbin/sshd-keygen**.

   d. Añade el parámetro **-f /etc/ssh/sshd-second_config** al comando **sshd**, para que se utilice el archivo de configuración alternativo:

   ```
   ExecStart=/usr/sbin/sshd -D -f /etc/sshd-second_config $OPTIONS
   ```

   e. Después de las modificaciones anteriores, el sshd-second.service debería tener el siguiente aspecto:

   ```
   [Unit]
   Description=OpenSSH server second instance daemon
   After=syslog.target network.target auditd.service sshd.service

   [Service]
   EnvironmentFile=/etc/sysconfig/sshd
   ExecStart=/usr/sbin/sshd -D -f /etc/ssh/sshd-second_config $OPTIONS
   ExecReload=/bin/kill -HUP $MAINPID
   KillMode=process
   Restart=on-failure
   RestartSec=42s

   [Install]
   WantedBy=multi-user.target
   ```

5. Si utiliza SELinux, añada el puerto para la segunda instancia de sshd a los puertos SSH, de lo contrario la segunda instancia de sshd será rechazada para enlazar con el puerto:

   ```
   # semanage port -a -t ssh_port_t -p tcp 22220
   ```

6. Habilitar sshd-second.service, para que se inicie automáticamente al arrancar:

   ```
   # systemctl enable sshd-second.service
   ```

7. Compruebe si el servicio sshd-second.service se está ejecutando mediante el comando **systemctl status**.

8. Verifique si el puerto está habilitado correctamente conectándose al servicio:

   ```
   $ ssh -p 22220 user@server
   ```

Si el firewall está en uso, asegúrese de que está configurado adecuadamente para permitir las conexiones a la segunda instancia de sshd.

3.5.3.2. Elección de un objetivo para la ordenación y las dependencias de los archivos unitarios personalizados

Para aprender a elegir correctamente un objetivo para el ordenamiento y las dependencias de sus archivos de unidad personalizados, consulte los siguientes artículos:

- Cómo escribir un archivo de unidad de servicio que obliga a iniciar determinados servicios
- Cómo decidir qué dependencias debe tener la definición de una unidad de servicio systemd

Hay información adicional con algunos ejemplos reales de casos provocados por el orden y las dependencias en un archivo de unidad en el artículo de la Base de Conocimiento de Red Hat ¿Hay alguna información útil sobre la escritura de archivos de unidad?

Si desea establecer límites para los servicios iniciados por **systemd**, consulte el artículo de la Base de conocimientos de Red Hat Cómo establecer límites para los servicios en RHEL 7 y systemd. Estos límites deben establecerse en el archivo de unidad del servicio. Tenga en cuenta que **systemd** ignora los límites establecidos en los archivos de configuración **/etc/security/limits.conf** y **/etc/security/limits.d/*.conf**. Los límites definidos en estos archivos son establecidos por PAM cuando se inicia una sesión de inicio de sesión, pero los demonios iniciados por **systemd** no utilizan sesiones de inicio de sesión de PAM.

3.5.4. Conversión de los scripts de inicio de SysV en archivos de unidad

Antes de dedicar tiempo a convertir un script de init de SysV a un archivo de unidad, asegúrese de que la conversión no se haya hecho ya en otro lugar. Todos los servicios centrales instalados en Red Hat Enterprise Linux vienen con archivos de unidad por defecto, y lo mismo se aplica a muchos paquetes de software de terceros.

Convertir un script de init en un archivo de unidad requiere analizar el script y extraer la información necesaria del mismo. A partir de estos datos se puede crear un archivo de unidad. Como los scripts de init pueden variar enormemente según el tipo de servicio, es posible que tenga que emplear más opciones de configuración para la conversión que las que se describen en este capítulo. Tenga en cuenta que algunos niveles de personalización que estaban disponibles con los scripts init ya no son soportados por las unidades systemd.

La mayor parte de la información necesaria para la conversión se proporciona en la cabecera del script. El siguiente ejemplo muestra la sección inicial del script init utilizado para iniciar el servicio **postfix** en Red Hat Enterprise Linux 6:

```
!/bin/bash # postfix Postfix Mail Transfer Agent # chkconfig: 2345 80 30 # description: Postfix is a Mail Transport Agent, which is the program that moves mail from one machine to another. # processname: master # pidfile: /var/spool/postfix/pid/master.pid # config: /etc/postfix/main.cf # config: /etc/postfix/master.cf  BEGIN INIT INFO # Provides: postfix MTA # Required-Start: $local_fs $network $remote_fs # Required-Stop: $local_fs $network $remote_fs # Default-Start: 2 3 4 5 # Default-Stop: 0 1 6 # Short-Description: start and stop postfix # Description: Postfix is a Mail Transport Agent, which is the program that moves mail from one machine to another. # END INIT INFO
```

En el ejemplo anterior, sólo las líneas que comienzan con **# chkconfig** y **# description** son obligatorias, por lo que es posible que no encuentre el resto en diferentes archivos init. El texto encerrado entre las líneas **BEGIN INIT INFO** y **END INIT INFO** se llama **Linux Standard Base (LSB) header**. Si se especifica, las cabeceras LSB contienen directivas que definen la descripción del servicio, las

dependencias y los niveles de ejecución por defecto. Lo que sigue es un resumen de las tareas analíticas destinadas a recopilar los datos necesarios para un nuevo archivo de unidad. Se utiliza como ejemplo el script init de postfix.

3.5.4.1. Encontrar la descripción del servicio systemd

Puede encontrar información descriptiva sobre el script en la línea que comienza con **#description**. Utilice esta descripción junto con el nombre del servicio en la opción **Description** en la sección [Unidad] del archivo de unidad. La cabecera LSB puede contener datos similares en las líneas **#Short-Description** y **#Description**.

3.5.4.2. Encontrar las dependencias del servicio systemd

La cabecera LSB puede contener varias directivas que forman dependencias entre servicios. La mayoría de ellas son traducibles a las opciones de la unidad systemd, véase Tabla 3.12, "Opciones de dependencia de la cabecera LSB"

Tabla 3.12. Opciones de dependencia de la cabecera LSB

Opción LSB	Descripción	Fichero de unidades equivalente
Provides	Especifica el nombre de la instalación de arranque del servicio, que puede ser referenciado en otros scripts de init (con el prefijo "$"). Esto ya no es necesario, ya que los archivos de unidad hacen referencia a otras unidades por sus nombres de archivo.	- -
Required-Start	Contiene los nombres de las instalaciones de arranque de los servicios requeridos. Esto se traduce como una dependencia de ordenación, los nombres de las instalaciones de arranque se sustituyen por los nombres de los archivos de unidad de los servicios correspondientes o los objetivos a los que pertenecen. Por ejemplo, en el caso de **postfix**, la dependencia Required-Start de $network se tradujo a la dependencia After de network.target.	**After**, **Before**
Should-Start	Constituye dependencias más débiles que Required-Start. Las dependencias Should-Start fallidas no afectan al inicio del servicio.	**After**, **Before**

Opción LSB	Descripción	Fichero de unidades equivalente
Required-Stop, **Should-Stop**	Constituye una dependencia negativa.	**Conflicts**

3.5.4.3. Encontrar los objetivos por defecto del servicio

La línea que comienza con **#chkconfig** contiene tres valores numéricos. El más importante es el primer número que representa los niveles de ejecución por defecto en los que se inicia el servicio. Asigne estos niveles de ejecución a objetivos systemd equivalentes. A continuación, enumere estos objetivos en la opción **WantedBy** de la sección [Install] del archivo de unidad. Por ejemplo, **postfix** se inició previamente en los niveles de ejecución 2, 3, 4 y 5, lo que se traduce en multiuser.target y graphical.target. Tenga en cuenta que graphical.target depende de multiuser.target, por lo que no es necesario especificar ambos. Puede encontrar información sobre los niveles de ejecución predeterminados y prohibidos también en las líneas **#Default-Start** y **#Default-Stop** de la cabecera LSB.

Los otros dos valores especificados en la línea **#chkconfig** representan las prioridades de arranque y apagado del script init. Estos valores son interpretados por **systemd** si carga el script de init, pero no hay un archivo de unidad equivalente.

3.5.4.4. Búsqueda de archivos utilizados por el servicio

Los scripts de inicio requieren la carga de una biblioteca de funciones desde un directorio dedicado y permiten importar archivos de configuración, entorno y PID. Las variables de entorno se especifican en la línea que comienza con **#config** en la cabecera del script de init, que se traduce en la opción de archivo de unidad **EnvironmentFile**. El archivo PID especificado en la línea del script de inicio **#pidfile** se importa al archivo de unidad con la opción **PIDFile**.

La información clave que no se incluye en la cabecera del script de init es la ruta al ejecutable del servicio, y potencialmente algunos otros archivos requeridos por el servicio. En versiones anteriores de Red Hat Enterprise Linux, los scripts de init utilizaban una sentencia case de Bash para definir el comportamiento del servicio en acciones predeterminadas, tales como **start**, **stop**, o **restart**, así como acciones definidas por el usuario. El siguiente extracto del script de init **postfix** muestra el bloque de código que se ejecuta al iniciar el servicio.

```
conf_check() {
    [ -x /usr/sbin/postfix ] || exit 5
    [ -d /etc/postfix ] || exit 6
    [ -d /var/spool/postfix ] || exit 5
}

make_aliasesdb() {
 if [ "$(/usr/sbin/postconf -h alias_database)" == "hash:/etc/aliases" ]
 then
  # /etc/aliases.db might be used by other MTA, make sure nothing
  # has touched it since our last newaliases call
  [ /etc/aliases -nt /etc/aliases.db ] ||
   [ "$ALIASESDB_STAMP" -nt /etc/aliases.db ] ||
   [ "$ALIASESDB_STAMP" -ot /etc/aliases.db ] || return
  /usr/bin/newaliases
  touch -r /etc/aliases.db "$ALIASESDB_STAMP"
 else
  /usr/bin/newaliases
```

```
 fi
}

start() {
 [ "$EUID" != "0" ] && exit 4
 # Check that networking is up.
 [ ${NETWORKING} = "no" ] && exit 1
 conf_check
 # Start daemons.
 echo -n $"Starting postfix: "
 make_aliasesdb >/dev/null 2>&1
 [ -x $CHROOT_UPDATE ] && $CHROOT_UPDATE
 /usr/sbin/postfix start 2>/dev/null 1>&2 && success || failure $"$prog start"
 RETVAL=$?
 [ $RETVAL -eq 0 ] && touch $lockfile
        echo
 return $RETVAL
}
```

La extensibilidad del script init permitió especificar dos funciones personalizadas, **conf_check()** y **make_aliasesdb()**, que se llaman desde el bloque de funciones **start()**. En el código anterior se mencionan varios archivos y directorios externos: el ejecutable del servicio principal **/usr/sbin/postfix**, los directorios de configuración **/etc/postfix/** y **/var/spool/postfix/**, así como el directorio **/usr/sbin/postconf/**.

Systemd sólo admite las acciones predefinidas, pero permite ejecutar ejecutables personalizados con las opciones **ExecStart**, **ExecStartPre**, **ExecStartPost**, **ExecStop** y **ExecReload**. El **/usr/sbin/postfix** junto con los scripts de apoyo se ejecutan al iniciar el servicio. La conversión de scripts init complejos requiere entender el propósito de cada declaración en el script. Algunas de las sentencias son específicas de la versión del sistema operativo, por lo que no es necesario traducirlas. Por otro lado, pueden ser necesarios algunos ajustes en el nuevo entorno, tanto en el archivo de unidad como en el ejecutable del servicio y los archivos de apoyo.

3.5.5. Modificación de archivos de unidad existentes

Los servicios instalados en el sistema vienen con archivos de unidad por defecto que se almacenan en el directorio **/usr/lib/systemd/system/**. Los administradores del sistema no deben modificar estos archivos directamente, por lo que cualquier personalización debe limitarse a los archivos de configuración en el directorio **/etc/systemd/system/**.

Procedimiento

1. Dependiendo del alcance de los cambios requeridos, elija uno de los siguientes enfoques:

   - Cree un directorio para los archivos de configuración suplementarios en **/etc/systemd/system/*unit*.d/**. Este método se recomienda para la mayoría de los casos de uso. Permite ampliar la configuración por defecto con funcionalidades adicionales, sin dejar de hacer referencia al archivo de unidad original. Por lo tanto, los cambios en la unidad por defecto introducidos con una actualización del paquete se aplican automáticamente. Consulte Ampliar la configuración de la unidad por defecto para obtener más información.

   - Cree una copia del archivo original de la unidad **/usr/lib/systemd/system/** en **/etc/systemd/system/** y realice los cambios allí. La copia anula el archivo original, por lo que los cambios introducidos con la actualización del paquete no se aplican. Este método es útil

para realizar cambios significativos en las unidades que deben persistir independientemente de las actualizaciones del paquete. Consulte Anulación de la configuración de la unidad por defecto para más detalles.

2. Para volver a la configuración por defecto de la unidad, borre los archivos de configuración creados a medida en **/etc/systemd/system/**.

3. Para aplicar los cambios en los archivos de la unidad sin reiniciar el sistema, ejecute

```
systemctl daemon-reload
```

La opción **daemon-reload** recarga todos los archivos de unidad y recrea todo el árbol de dependencias, lo cual es necesario para aplicar inmediatamente cualquier cambio en un archivo de unidad. Como alternativa, puede lograr el mismo resultado con el siguiente comando, que debe ejecutarse bajo el usuario **root**:

```
init q
```

4. Si el archivo de unidad modificado pertenece a un servicio en ejecución, este servicio debe reiniciarse para aceptar la nueva configuración:

```
systemctl restart name.service
```

IMPORTANTE

Para modificar las propiedades, como las dependencias o los tiempos de espera, de un servicio gestionado por un initscript de SysV, no modifique el propio initscript. En su lugar, cree un archivo de configuración drop-in **systemd** para el servicio como se describe en Ampliación de la configuración de la unidad por defecto y Anulación de la configuración de la unidad por defecto. A continuación, gestione este servicio de la misma manera que un servicio normal de **systemd**.

Por ejemplo, para ampliar la configuración del servicio **network**, no modifique el archivo initscript **/etc/rc.d/init.d/network**. En su lugar, cree un nuevo directorio **/etc/systemd/system/network.service.d/** y un archivo drop-in **systemd /etc/systemd/system/network.service.d/*my_config*.conf**. A continuación, introduzca los valores modificados en el archivo drop-in. Nota: **systemd** conoce el servicio **network** como **network.service**, por lo que el directorio creado debe llamarse **network.service.d**

3.5.5.1. Ampliación de la configuración de la unidad por defecto

Esta sección describe cómo ampliar el archivo de unidad por defecto con opciones de configuración adicionales.

Procedimiento

1. Para ampliar el archivo de unidad por defecto con opciones de configuración adicionales, cree primero un directorio de configuración en **/etc/systemd/system/**. Si se amplía una unidad de servicio, ejecute el siguiente comando como **root**:

```
mkdir /etc/systemd/system/name.service.d/
```

Sustituya *name* por el nombre del servicio que desea ampliar. La sintaxis anterior se aplica a todos los tipos de unidades.

2. Cree un archivo de configuración en el directorio creado en el paso anterior. Tenga en cuenta que el nombre del archivo debe terminar con el sufijo **.conf**. Escriba:

```
tocar /etc/systemd/system/name.service.d/config_name.conf
```

Sustituya *config_name* por el nombre del archivo de configuración. Este archivo se adhiere a la estructura normal de los archivos de la unidad, por lo que todas las directivas deben ser especificadas en las secciones apropiadas, ver Estructura de los archivos de la unidad .

Por ejemplo, para añadir una dependencia personalizada, cree un archivo de configuración con el siguiente contenido:

```
[Unit]
Requires=new_dependency
After=new_dependency
```

Donde *new_dependency* representa la unidad que debe marcarse como dependencia. Otro ejemplo es un archivo de configuración que reinicia el servicio después de la salida de su proceso principal, con un retraso de 30 segundos:

```
[Service]
Restart=always
RestartSec=30
```

Se recomienda crear pequeños archivos de configuración centrados sólo en una tarea. Dichos archivos se pueden mover o enlazar fácilmente a los directorios de configuración de otros servicios.

3. Para aplicar los cambios realizados en la unidad, ejecute como **root**:

```
systemctl daemon-reload
systemctl restart name.service
```

Ejemplo 3.10. Ampliación de la configuración de httpd.service

Para modificar la unidad httpd.service de forma que se ejecute automáticamente un script de shell personalizado al iniciar el servicio Apache, realice los siguientes pasos.

1. Cree un directorio y un archivo de configuración personalizado:

```
# mkdir /etc/systemd/system/httpd.service.d/
```

```
# touch /etc/systemd/system/httpd.service.d/custom_script.conf
```

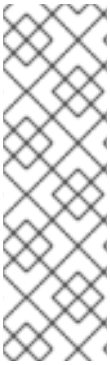
2. Siempre que el script que desea iniciar automáticamente con Apache se encuentre en **/usr/local/bin/custom.sh**, inserte el siguiente texto en el archivo **custom_script.conf**:

```
[Service]
ExecStartPost=/usr/local/bin/custom.sh
```

3. Para aplicar los cambios de la unidad, ejecute:

```
# systemctl daemon-reload
```

```
# systemctl restart httpd.service
```



NOTA

Los archivos de configuración de los directorios de configuración en **/etc/systemd/system/** tienen prioridad sobre los archivos de unidad en **/usr/lib/systemd/system/**. Por lo tanto, si los archivos de configuración contienen una opción que sólo puede especificarse una vez, como **Description** o **ExecStart**, se anula el valor por defecto de esta opción. Tenga en cuenta que en la salida del comando **systemd-delta**, descrita en Monitoreo de unidades anuladas, tales unidades están siempre marcadas como [EXTENDED], aunque en suma, ciertas opciones son realmente anuladas.

3.5.5.2. Anulación de la configuración de la unidad por defecto

Esta sección describe cómo anular la configuración por defecto de la unidad.

Procedimiento

1. Para realizar cambios que persistan después de actualizar el paquete que proporciona el archivo de la unidad, copie primero el archivo en el directorio **/etc/systemd/system/**. Para ello, ejecute el siguiente comando como **root**:

   ```
   cp /usr/lib/systemd/system/name.service /etc/systemd/system/name.service
   ```

   Donde *name* representa el nombre de la unidad de servicio que desea modificar. La sintaxis anterior se aplica a todos los tipos de unidades.

2. Abra el archivo copiado con un editor de texto y realice los cambios deseados. Para aplicar los cambios de la unidad, ejecute como **root**:

   ```
   systemctl daemon-reload
   systemctl restart name.service
   ```

Ejemplo 3.11. Cambiar el límite de tiempo de espera

Puede especificar un valor de tiempo de espera por servicio para evitar que un servicio que funcione mal congele el sistema. De lo contrario, el tiempo de espera se establece por defecto en 90 segundos para los servicios normales y en 300 segundos para los servicios compatibles con SysV.

Por ejemplo, para ampliar el límite de tiempo de espera del servicio **httpd**:

1. Copie el archivo de la unidad **httpd** en el directorio **/etc/systemd/system/**:

   ```
   cp /usr/lib/systemd/system/httpd.service /etc/systemd/system/httpd.service
   ```

2. Abra el archivo **/etc/systemd/system/httpd.service** y especifique el valor de **TimeoutStartUSec** en la sección **[Service]**:

   ```
   …
   [Service]
   …
   ```

```
PrivateTmp=true
TimeoutStartSec=10

[Install]
WantedBy=multi-user.target
…
```

3. Recarga el demonio **systemd**:

```
systemctl daemon-reload
```

4. **Optional.** Verifique el nuevo valor del tiempo de espera:

```
systemctl show httpd -p TimeoutStartUSec
```

NOTA

Para cambiar el límite de tiempo de espera globalmente, introduzca el **DefaultTimeoutStartSec** en el archivo **/etc/systemd/system.conf**.

3.5.5.3. Control de las unidades anuladas

Esta sección describe cómo mostrar un resumen de los archivos de unidad anulados o modificados.

Procedimiento

1. Para mostrar un resumen de los archivos de unidad anulados o modificados, utilice el siguiente comando:

```
systemd-delta
```

Por ejemplo, la salida del comando anterior puede tener el siguiente aspecto:

```
[EQUIVALENT] /etc/systemd/system/default.target → /usr/lib/systemd/system/default.target
[OVERRIDDEN] /etc/systemd/system/autofs.service →
/usr/lib/systemd/system/autofs.service

--- /usr/lib/systemd/system/autofs.service      2014-10-16 21:30:39.000000000 -0400
+ /etc/systemd/system/autofs.service  2014-11-21 10:00:58.513568275 -0500
@@ -8,7 +8,8 @@
 EnvironmentFile=-/etc/sysconfig/autofs
 ExecStart=/usr/sbin/automount $OPTIONS --pid-file /run/autofs.pid
 ExecReload=/usr/bin/kill -HUP $MAINPID
-TimeoutSec=180
+TimeoutSec=240
+Restart=Always

 [Install]
 WantedBy=multi-user.target

[MASKED]     /etc/systemd/system/cups.service → /usr/lib/systemd/system/cups.service
[EXTENDED]   /usr/lib/systemd/system/sssd.service →
```

```
/etc/systemd/system/sssd.service.d/journal.conf

4 overridden configuration files found.
```

3.5.6. Trabajar con unidades instanciadas

Es posible instanciar múltiples unidades desde un único archivo de configuración de plantilla en tiempo de ejecución. El carácter "@" se utiliza para marcar la plantilla y asociar las unidades con ella. Las unidades instanciadas pueden iniciarse desde otro archivo de unidades (utilizando las opciones **Requires** o **Wants**), o con el comando **systemctl start**. Las unidades de servicio instanciadas se nombran de la siguiente manera:

```
template_name@instance_name.service
```

Donde *template_name* representa el nombre del archivo de configuración de la plantilla. Sustituya *instance_name* por el nombre de la instancia de la unidad. Varias instancias pueden apuntar al mismo archivo de plantilla con opciones de configuración comunes para todas las instancias de la unidad. El nombre de la unidad de plantilla tiene la forma de:

```
unit_name@.service
```

Por ejemplo, la siguiente configuración de **Wants** en un archivo de unidad:

```
Wants=getty@ttyA.service getty@ttyB.service
```

primero hace que systemd busque las unidades de servicio dadas. Si no se encuentran tales unidades, la parte entre "@" y el sufijo de tipo se ignora y **systemd** busca el archivo **getty@.service**, lee la configuración de éste y arranca los servicios.

Por ejemplo, la plantilla **getty@.service** contiene las siguientes directivas:

```
[Unit]
Description=Getty on %I
…
[Service]
ExecStart=-/sbin/agetty --noclear %I $TERM
…
```

Cuando se instancian getty@ttyA.service y getty@ttyB.service desde la plantilla anterior, **Description**= se resuelve como **Getty on ttyA** y **Getty on ttyB**.

3.5.6.1. Especificaciones importantes de las unidades

Los caracteres comodín, denominados **unit specifiers**, pueden utilizarse en cualquier archivo de configuración de unidades. Los especificadores de unidad sustituyen ciertos parámetros de la unidad y se interpretan en tiempo de ejecución. Tabla 3.13, “Especificaciones importantes de las unidades” enumera los especificadores de unidad que son particularmente útiles para las unidades de plantilla.

Tabla 3.13. Especificaciones importantes de las unidades

Especificador de unidades	Significado	Descripción

Especificador de unidades	Significado	Descripción
%n	Nombre completo de la unidad	Representa el nombre completo de la unidad, incluido el sufijo de tipo. **%N** tiene el mismo significado, pero también sustituye los caracteres prohibidos por códigos ASCII.
%p	Nombre del prefijo	Representa un nombre de unidad con el sufijo de tipo eliminado. Para las unidades instanciadas, %p representa la parte del nombre de la unidad antes del carácter "@".
%i	Nombre de la instancia	Es la parte del nombre de la unidad instanciada entre el carácter "@" y el sufijo de tipo. **%I** tiene el mismo significado pero también sustituye a los caracteres prohibidos para los códigos ASCII.
%H	Nombre del anfitrión	Representa el nombre de host del sistema en ejecución en el momento en que se carga la configuración de la unidad.
%t	Directorio de tiempo de ejecución	Representa el directorio de tiempo de ejecución, que es /**run** para el usuario **root**, o el valor de la variable XDG_RUNTIME_DIR para los usuarios sin privilegios.

Para obtener una lista completa de especificadores de unidades, consulte la página del manual **systemd.unit(5)**.

3.6. OPTIMIZACIÓN DE SYSTEMD PARA ACORTAR EL TIEMPO DE ARRANQUE

Hay una lista de archivos de unidad systemd que están activados por defecto. Los servicios del sistema definidos por estos archivos de unidad se ejecutan automáticamente en el arranque, lo que influye en el tiempo de arranque.

Esta sección describe:

- Las herramientas para examinar el rendimiento del arranque del sistema.

- El propósito de las unidades de systemd habilitadas por defecto, y las circunstancias en las que se puede deshabilitar de forma segura dichas unidades de systemd con el fin de acortar el tiempo de arranque.

3.6.1. Examinar el rendimiento de arranque del sistema

Para examinar el rendimiento del arranque del sistema, puede utilizar el comando **systemd-analyze**. Este comando tiene muchas opciones disponibles. Sin embargo, esta sección cubre sólo las seleccionadas que pueden ser importantes para el ajuste de systemd con el fin de acortar el tiempo de arranque.

Para obtener una lista completa y una descripción detallada de todas las opciones, consulte la página man **systemd-analyze**.

Requisitos previos

Antes de empezar a examinar systemd para afinar el tiempo de arranque, es posible que quieras listar todos los servicios habilitados:

```
$ systemctl list-unit-files --state=enabled
```

Analizar el tiempo total de arranque

Procedimiento

- Para obtener la información general sobre el tiempo que duró el último arranque con éxito, utilice:

```
$ systemd-analyze
```

Analizar el tiempo de inicialización de la unidad

Procedimiento

- Para obtener información sobre el tiempo de inicialización de cada unidad systemd, utilice

```
$ systemd-analyze blame
```

La salida enumera las unidades en orden descendente según el tiempo que tardaron en inicializarse durante el último arranque con éxito.

Identificación de unidades críticas

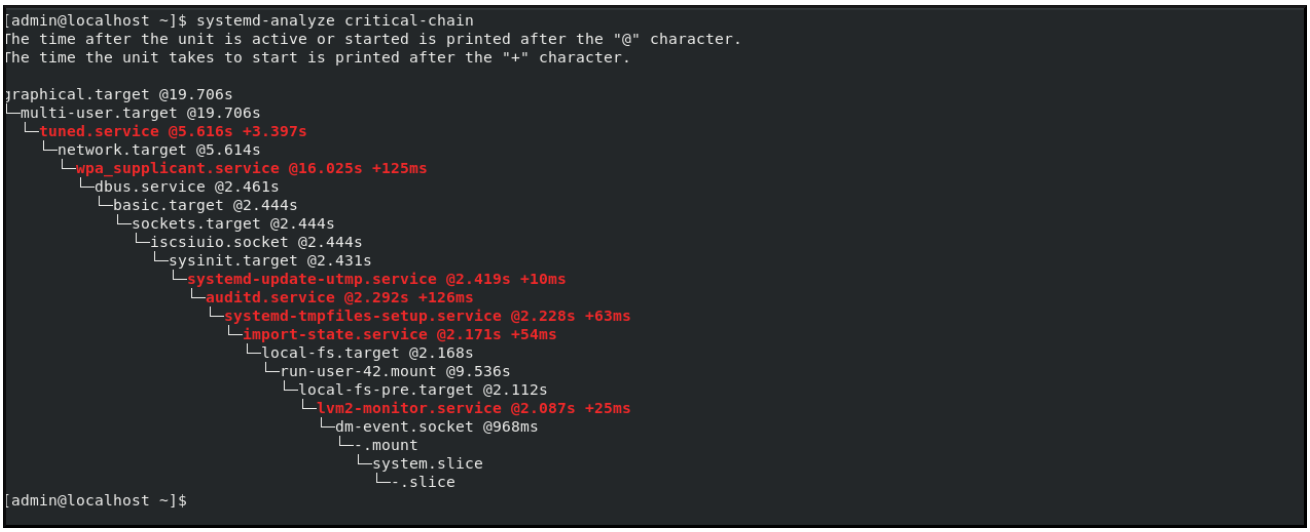
Procedimiento

- Para identificar las unidades que tardaron más tiempo en inicializarse en el último arranque con éxito, utilice:

```
$ systemd-analyze critical-chain
```

La salida destaca las unidades que ralentizan críticamente el arranque con el color rojo.

Figura 3.1. La salida del comando systemd-analyze critical-chain



3.6.2. Una guía para seleccionar los servicios que se pueden desactivar con seguridad

Si el tiempo de arranque de tu sistema es largo, puedes acortarlo deshabilitando algunos de los servicios habilitados por defecto en el arranque.

Para listar estos servicios, ejecute:

```
$ systemctl list-unit-files --state=enabled
```

Para desactivar un servicio, ejecute:

```
# systemctl disable service_name
```

Sin embargo, ciertos servicios deben permanecer activados para que su sistema operativo sea seguro y funcione de la manera que usted necesita.

Puede utilizar la tabla siguiente como una guía para seleccionar los servicios que puede deshabilitar de forma segura. La tabla enumera todos los servicios habilitados por defecto en una instalación mínima de Red Hat Enterprise Linux 8, y para cada servicio indica si este servicio puede ser deshabilitado de forma segura.

La tabla también proporciona más información sobre las circunstancias en las que se puede desactivar el servicio, o la razón por la que no se debe desactivar el servicio.

Tabla 3.14. Servicios habilitados por defecto en una instalación mínima de RHEL 8

Nombre del servicio	¿Se puede desactivar?	Más información

Nombre del servicio	¿Se puede desactivar?	Más información
auditd.service	sí	Desactive **auditd.service** sólo si no necesita mensajes de auditoría del kernel. Tenga en cuenta que si desactiva **auditd.service**, el archivo **/var/log/audit/audit.log** no se produce. En consecuencia, no podrá revisar retroactivamente algunas acciones o eventos comúnmente revisados, como los inicios de sesión de los usuarios, los arranques de los servicios o los cambios de contraseña. También tenga en cuenta que auditd tiene dos partes: una parte del kernel y un servicio propio. Al utilizar el comando **systemctl disable auditd**, sólo se desactiva el servicio, pero no la parte del kernel. Para desactivar la auditoría del sistema en su totalidad, establezca **audit=0** en la línea de comandos del kernel.
autovt@.service	no	Este servicio se ejecuta sólo cuando es realmente necesario, por lo que no es necesario desactivarlo.
servicio.crond	sí	Tenga en cuenta que ningún elemento de crontab se ejecutará si desactiva crond.service.
dbus-org.fedoraproject.FirewallD1.service	sí	Un enlace simbólico a **firewalld.service**
dbus-org.freedesktop.NetworkManager.service	sí	Un enlace simbólico a **NetworkManager.service**
dbus-org.freedesktop.nm-dispatcher.service	sí	Un enlace simbólico a **NetworkManager-dispatcher.service**
firewalld.service	sí	Desactive **firewalld.service** sólo si no necesita un cortafuegos.

Nombre del servicio	¿Se puede desactivar?	Más información
getty@.service	no	Este servicio se ejecuta sólo cuando es realmente necesario, por lo que no es necesario desactivarlo.
servicio.de.importación	sí	Desactive **import-state.service** sólo si no necesita arrancar desde un almacenamiento en red.
irqbalance.service	sí	Desactive **irqbalance.service** sólo si tiene una sola CPU. No desactive **irqbalance.service** en sistemas con múltiples CPUs.
kdump.service	sí	Desactive **kdump.service** sólo si no necesita los informes de las caídas del kernel.
loadmodules.service	sí	Este servicio no se inicia a menos que exista el directorio **/etc/rc.modules** o **/etc/sysconfig/modules**, lo que significa que no se inicia en una instalación mínima de RHEL 8.
lvm2-monitor.service	sí	Desactive **lvm2-monitor.service** sólo si no utiliza Logical Volume Manager (LVM).
microcode.service	no	No se desactive el servicio porque proporciona actualizaciones del software de microcódigo en la CPU.
NetworkManager-dispatcher.service	sí	Desactive **NetworkManager-dispatcher.service** sólo si no necesita notificaciones sobre cambios en la configuración de la red (por ejemplo, en redes estáticas).

Nombre del servicio	¿Se puede desactivar?	Más información
NetworkManager-wait-online.service	sí	Desactive **NetworkManager-wait-online.service** sólo si no necesita que la conexión de red funcione justo después del arranque. Si el servicio está habilitado, el sistema no termina el arranque antes de que la conexión de red esté funcionando. Esto puede prolongar significativamente el tiempo de arranque.
NetworkManager.service	sí	Desactive **NetworkManager.service** sólo si no necesita conectarse a una red.
nis-nombre-dominio.servicio	sí	Desactive **nis-domainname.service** sólo si no utiliza el Servicio de Información de Red (NIS).
rhsmcertd.service	no	
rngd.service	sí	Desactiva **rngd.service** sólo si no necesitas mucha entropía en tu sistema, o no tienes ningún tipo de generador de hardware. Tenga en cuenta que el servicio es necesario en entornos que requieren mucha y buena entropía, como los sistemas utilizados para la generación de certificados X.509 (por ejemplo el servidor FreeIPA).
rsyslog.service	sí	Desactive **rsyslog.service** sólo si no necesita registros persistentes, o si configura **systemd-journald** en modo persistente.
selinux-autorelabel-mark.service	sí	Desactive **selinux-autorelabel-mark.service** sólo si no utiliza SELinux.

Nombre del servicio	¿Se puede desactivar?	Más información
sshd.service	sí	Desactive **sshd.service** sólo si no necesita inicios de sesión remotos por parte del servidor OpenSSH.
sssd.service	sí	Desactive **sssd.service** sólo si no hay usuarios que se registren en el sistema a través de la red (por ejemplo, utilizando LDAP o Kerberos). Red Hat recomienda desactivar todas las unidades de **sssd-*** si se desactiva **sssd.service**.
syslog.service	sí	Un alias para **rsyslog.service**
tuned.service	sí	Desactive **tuned.service** sólo si necesita utilizar el ajuste de rendimiento.
lvm2-lvmpolld.socket	sí	Desactive **lvm2-lvmpolld.socket** sólo si no utiliza Logical Volume Manager (LVM).
dnf-makecache.timer	sí	Desactive **dnf-makecache.timer** sólo si no necesita que los metadatos de sus paquetes se actualicen automáticamente.
anclaje-desatado.timer	sí	Desactive **unbound-anchor.timer** sólo si no necesita la actualización diaria del ancla de confianza raíz para las extensiones de seguridad del DNS (DNSSEC). Este ancla de confianza raíz es utilizada por el resolver y la biblioteca del resolver de Unbound para la validación de DNSSEC.

Para encontrar más información sobre un servicio, puede ejecutar uno de los siguientes comandos:

```
$ systemctl cat <nombre_del_servicio>
```

```
$ systemctl help <nombre_servicio>
```

El comando **systemctl cat** proporciona el contenido del archivo de servicio ubicado en **/usr/lib/systemd/system/<service>**, así como todas las anulaciones aplicables. Los overrides aplicables incluyen los overrides de los archivos de unidad del archivo **/etc/systemd/system/<service>** o los archivos drop-in de un directorio correspondiente de **unit.type.d**.

Para más información sobre los archivos drop-in, consulte la página man **systemd.unit**.

El comando **systemctl help** muestra la página man del servicio en cuestión.

3.7. RECURSOS ADICIONALES

Para más información sobre systemd y su uso en Red Hat Enterprise Linux, consulte los recursos listados a continuación.

3.7.1. Documentación instalada

- **systemctl**(1) - La página del manual de la utilidad de línea de comandos **systemctl** proporciona una lista completa de las opciones y comandos compatibles.
- **systemd**(1) - La página del manual del gestor de sistemas y servicios **systemd** proporciona más información sobre sus conceptos y documenta las opciones de la línea de comandos y las variables de entorno disponibles, los archivos y directorios de configuración soportados, las señales reconocidas y las opciones del kernel disponibles.
- **systemd-delta**(1) - La página del manual de la utilidad **systemd-delta** que permite encontrar archivos de configuración extendidos y anulados.
- **systemd.directives(7)** - La página del manual llamada **systemd.directives** proporciona información detallada sobre las directivas de systemd.
- **systemd.unit**(5) - La página del manual llamada **systemd.unit** proporciona información detallada sobre los archivos de la unidad systemd y documenta todas las opciones de configuración disponibles.
- **systemd.service**(5) - La página del manual denominada **systemd.service** documenta el formato de los archivos de las unidades de servicio.
- **systemd.target**(5) - La página del manual denominada **systemd.target** documenta el formato de los archivos de las unidades de destino.
- **systemd.kill**(5) - La página del manual denominada **systemd.kill** documenta la configuración del procedimiento de eliminación de procesos.

3.7.2. Documentación en línea

- página de inicio de systemd - La página de inicio del proyecto ofrece más información sobre systemd.

CAPÍTULO 4. INTRODUCCIÓN A LA GESTIÓN DE CUENTAS DE USUARIO Y DE GRUPO

El control de usuarios y grupos es un elemento central de la administración del sistema Red Hat Enterprise Linux (RHEL). Cada usuario de RHEL tiene credenciales de acceso distintas y puede ser asignado a varios grupos para personalizar sus privilegios en el sistema.

Un usuario que crea un archivo es el propietario de ese archivo *and* el propietario del grupo de ese archivo. Al archivo se le asignan permisos de lectura, escritura y ejecución separados para el propietario, el grupo y los que no pertenecen a ese grupo. El propietario del archivo sólo puede ser cambiado por el usuario **root**. Los permisos de acceso al archivo pueden ser cambiados tanto por el usuario **root** como por el propietario del archivo. Un usuario normal puede cambiar la propiedad de un archivo del que es propietario a un grupo del que es miembro.

Cada usuario está asociado a un número de identificación numérico único llamado *user ID* (**UID**). Cada grupo está asociado a un *group ID* (**GID**). Los usuarios de un grupo comparten los mismos permisos de lectura, escritura y ejecución de archivos que pertenecen a ese grupo.

4.1. INTRODUCCIÓN A LOS USUARIOS Y GRUPOS

Un usuario que crea un archivo es el propietario de ese archivo *and* el propietario del grupo de ese archivo. Al archivo se le asignan permisos de lectura, escritura y ejecución separados para el propietario, el grupo y los que no pertenecen a ese grupo. El propietario del archivo sólo puede ser cambiado por el usuario **root**. Los permisos de acceso al archivo pueden ser cambiados tanto por el usuario **root** como por el propietario del archivo. Un usuario normal puede cambiar la propiedad de un archivo del que es propietario a un grupo del que es miembro.

Cada usuario está asociado a un número de identificación numérico único llamado *user ID* (**UID**). Cada grupo está asociado a un *group ID* (**GID**). Los usuarios de un grupo comparten los mismos permisos de lectura, escritura y ejecución de archivos que pertenecen a ese grupo.

4.2. CONFIGURACIÓN DE IDS DE USUARIOS Y GRUPOS RESERVADOS

RHEL reserva los ID de usuario y grupo por debajo de 1000 para los usuarios y grupos del sistema. Puede encontrar los ID de usuario y grupo reservados en el paquete **setup**. Para ver los ID de usuario y grupo reservados, utilice:

```
cat /usr/share/doc/setup*/uidgid
```

Se recomienda asignar IDs a los nuevos usuarios y grupos a partir de 5000, ya que el rango reservado puede aumentar en el futuro.

Para que los IDs asignados a los nuevos usuarios comiencen en 5000 por defecto, modifique los parámetros **UID_MIN** y **GID_MIN** en el archivo **/etc/login.defs**.

Procedimiento

Para modificar hacer que los IDs asignados a los nuevos usuarios comiencen en 5000 por defecto, utilice:

1. Abra el archivo **/etc/login.defs** en un editor de su elección.
2. Encuentre las líneas que definen el valor mínimo para la selección automática de UID.

```
# Min/max values for automatic uid selection in useradd
#
UID_MIN                  1000
```

3. Modifica el valor de **UID_MIN** para que empiece en 5000.

```
# Min/max values for automatic uid selection in useradd
#
UID_MIN                  5000
```

4. Encuentre las líneas que definen el valor mínimo para la selección automática de GID.

```
# Min/max values for automatic gid selection in groupadd
#
GID_MIN                  1000
```

Tenga en cuenta que para los usuarios y grupos creados antes de cambiar los valores de **UID_MIN** y **GID_MIN**, los UIDs y GIDs siguen comenzando en el valor predeterminado de 1000.

AVISO

No aumente los IDs reservados por el sistema por encima de 1000 cambiando **SYS_UID_MAX** para evitar conflictos con los sistemas que mantienen el límite de 1000.

4.3. GRUPOS PRIVADOS DE USUARIOS

RHEL utiliza la configuración del sistema *user private group* (**UPG**), que facilita la gestión de los grupos UNIX. Cada vez que se añade un nuevo usuario al sistema se crea un grupo privado de usuarios. El grupo privado de usuarios tiene el mismo nombre que el usuario para el que fue creado y ese usuario es el único miembro del grupo privado de usuarios.

Las UPGs simplifican la colaboración en un proyecto entre múltiples usuarios. Además, la configuración del sistema UPG hace que sea seguro establecer permisos por defecto para un archivo o directorio recién creado, ya que permite tanto al usuario, como al grupo del que forma parte este usuario, realizar modificaciones en el archivo o directorio.

La lista de todos los grupos se almacena en el archivo de configuración **/etc/group**.

CAPÍTULO 5. GESTIÓN DE LAS CUENTAS DE USUARIO EN LA CONSOLA WEB

La consola web de RHEL ofrece una interfaz gráfica que le permite ejecutar una amplia gama de tareas administrativas sin tener que acceder directamente a su terminal. Por ejemplo, puede añadir, editar o eliminar cuentas de usuario del sistema.

Después de leer esta sección, lo sabrás:

- De donde provienen las cuentas existentes.
- Cómo añadir nuevas cuentas.
- Cómo establecer la caducidad de la contraseña.
- Cómo y cuándo terminar las sesiones de los usuarios.

Requisitos previos

- Configure la consola web de RHEL. Para más detalles, consulte Introducción al uso de la consola web de RHEL,
- Inicie sesión en la consola web de RHEL con una cuenta que tenga asignados permisos de administrador. Para obtener más detalles, consulte Iniciar sesión en la consola web de RHEL.

5.1. CUENTAS DE USUARIO DEL SISTEMA GESTIONADAS EN LA CONSOLA WEB

Con las cuentas de usuario que se muestran en la consola web de RHEL se puede:

- Autenticar a los usuarios al acceder al sistema.
- Establezca los derechos de acceso al sistema.

La consola web de RHEL muestra todas las cuentas de usuario ubicadas en el sistema. Por lo tanto, puede ver al menos una cuenta de usuario justo después del primer inicio de sesión en la consola web.

Después de iniciar sesión en la consola web de RHEL, puede realizar las siguientes operaciones:

- Crear nuevas cuentas de usuario.
- Cambia sus parámetros.
- Bloquea las cuentas.
- Terminar las sesiones de los usuarios.

5.2. AÑADIR NUEVAS CUENTAS MEDIANTE LA CONSOLA WEB

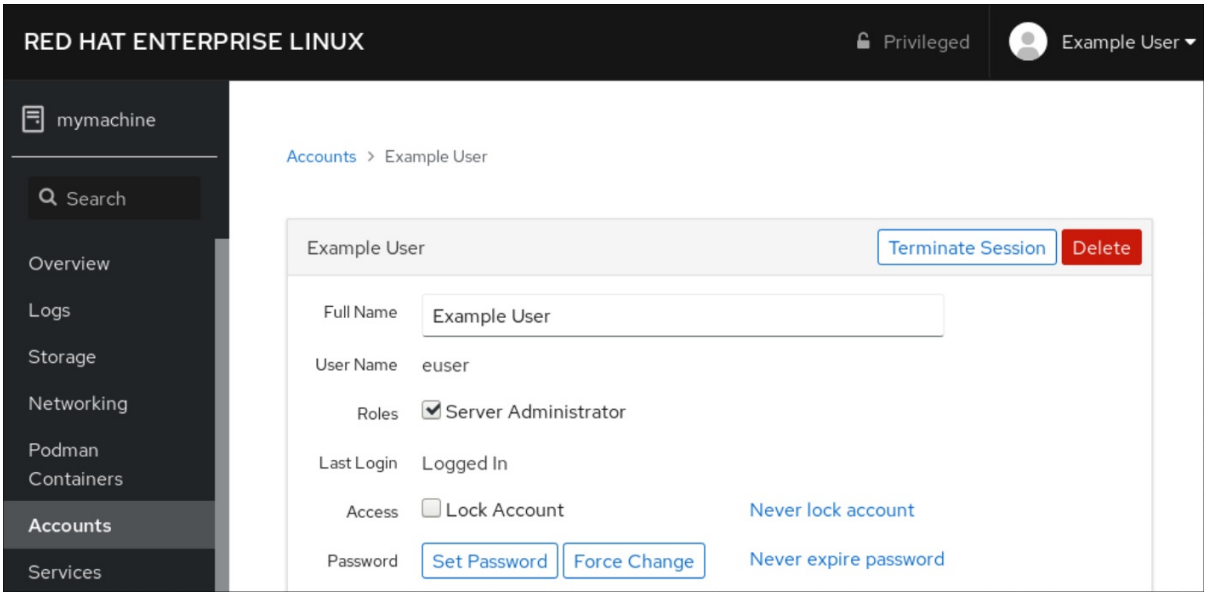
Siga los siguientes pasos para añadir cuentas de usuario al sistema y establecer los derechos de administración de las cuentas a través de la consola web de RHEL.

Requisitos previos

- La consola web de RHEL debe estar instalada y accesible. Para más detalles, consulte Instalación de la consola web.

Procedimiento

1. Inicie sesión en la consola web de RHEL.
2. Haga clic en **Cuentas**.
3. Haga clic en **Crear una nueva cuenta**.
1. En el campo **Full Name**, introduzca el nombre completo del usuario.
   La consola web de RHEL sugiere automáticamente un nombre de usuario a partir del nombre completo y lo rellena en el campo **User Name**. Si no desea utilizar la convención de nomenclatura original que consiste en la primera letra del nombre y el apellido completo, actualice la sugerencia.
2. En los campos de **Password/Confirm**, introduzca la contraseña y vuelva a escribirla para verificar que es correcta.
   La barra de color situada debajo de los campos muestra el nivel de seguridad de la contraseña introducida, lo que no permite crear un usuario con una contraseña débil.
1. Haga clic en **Crear** para guardar la configuración y cerrar el cuadro de diálogo.
2. Seleccione la cuenta recién creada.
3. Seleccione **Server Administrator** en el elemento **Roles**.



Ahora puede ver la nueva cuenta en la configuración de **Accounts** y puede utilizar las credenciales para conectarse al sistema.

5.3. APLICACIÓN DE LA CADUCIDAD DE LA CONTRASEÑA EN LA CONSOLA WEB

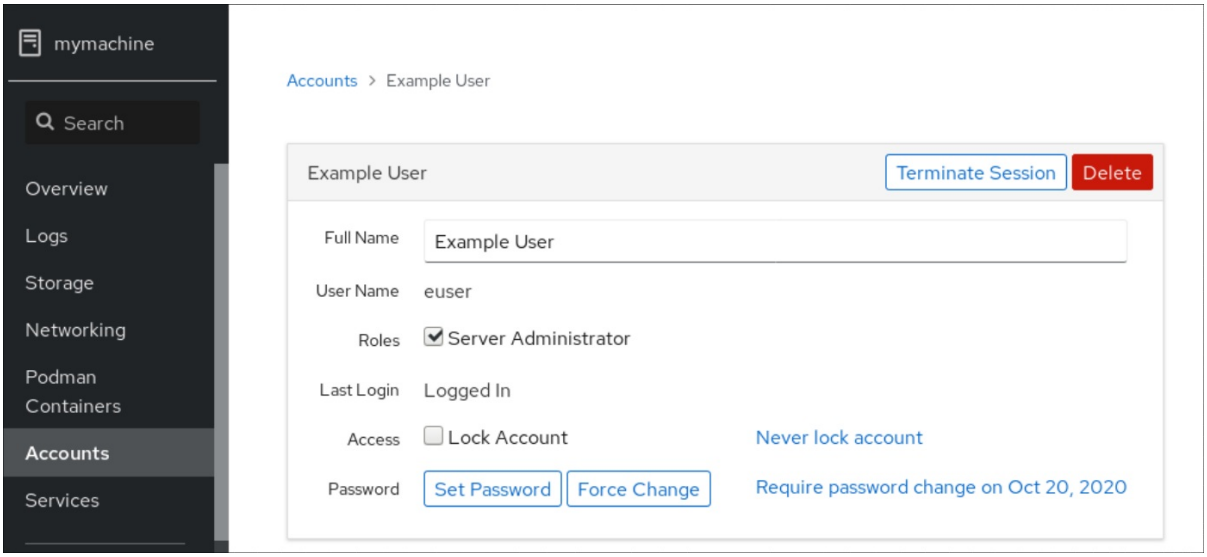
Por defecto, las cuentas de usuario tienen establecidas contraseñas que no caducan nunca. Puede configurar las contraseñas del sistema para que caduquen después de un número determinado de días. Cuando la contraseña caduque, el siguiente intento de inicio de sesión solicitará un cambio de contraseña.

Procedimiento

1. Inicie sesión en la consola web de RHEL 8.
2. Haga clic en **Cuentas**.
3. Seleccione la cuenta de usuario para la que se va a imponer la caducidad de la contraseña.
4. En la configuración de la cuenta de usuario, haga clic en **No caducar nunca la contraseña**.
5. En el cuadro de diálogo **Password Expiration**, seleccione **Require password change every ... days** e introduzca un número entero positivo que represente el número de días en que caduca la contraseña.
1. Haga clic en **Cambiar**.

Pasos de verificación

- Para comprobar que la caducidad de la contraseña está configurada, abra la configuración de la cuenta.
  La consola web de RHEL 8 muestra un enlace con la fecha de caducidad.



5.4. TERMINAR LAS SESIONES DE LOS USUARIOS EN LA CONSOLA WEB

Un usuario crea sesiones de usuario cuando se conecta al sistema. Terminar las sesiones de usuario significa cerrar la sesión del usuario en el sistema. Puede ser útil si necesita realizar tareas administrativas sensibles a los cambios de configuración, por ejemplo, actualizaciones del sistema.

En cada cuenta de usuario de la consola web de RHEL 8, puede finalizar todas las sesiones de la cuenta, excepto la sesión de la consola web que esté utilizando en ese momento. Esto evita que pierdas el acceso a tu sistema.

Procedimiento

1. Inicie sesión en la consola web de RHEL 8.
2. Haga clic en **Cuentas**.

3. Haga clic en la cuenta de usuario para la que desea terminar la sesión.

4. Haga clic en **Terminar Sesión**.
   Si el botón de **Terminar Sesión** está inactivo, el usuario no está conectado al sistema.

   La consola web de RHEL termina las sesiones.

CAPÍTULO 6. GESTIÓN DE USUARIOS DESDE LA LÍNEA DE COMANDOS

Puede gestionar usuarios y grupos utilizando la interfaz de línea de comandos (**CLI**). Esto le permite añadir, eliminar y modificar usuarios y grupos de usuarios en el entorno de Red Hat Enterprise Linux.

6.1. AÑADIR UN NUEVO USUARIO DESDE LA LÍNEA DE COMANDOS

Esta sección describe cómo utilizar la utilidad **useradd** para añadir un nuevo usuario.

Requisitos previos

- **Root** acceso

Procedimiento

- Para añadir un nuevo usuario, utilice:

```
# useradd options username
```

Sustituya *options* por las opciones de la línea de comandos para el comando **useradd**, y sustituya *username* por el nombre del usuario.

Ejemplo 6.1. Añadir un nuevo usuario

Para añadir el usuario **sarah** con el ID de usuario **5000**, utilice:

```
# useradd -u 5000 sarah
```

Pasos de verificación

- Para comprobar que el nuevo usuario se ha añadido, utilice la utilidad **id**.

```
# id sarah
```

La salida devuelve:

```
uid=5000(sarah) gid=5000(sarah) groups=5000(sarah)
```

Recursos adicionales

- **useradd** página de manual

6.2. AÑADIR UN NUEVO GRUPO DESDE LA LÍNEA DE COMANDOS

Esta sección describe cómo utilizar la utilidad **groupadd** para añadir un nuevo grupo.

Requisitos previos

- **Root** acceso

Procedimiento

- Para añadir un nuevo grupo, utilice:

```
# groupadd options group-name
```

Sustituya *options* por las opciones de la línea de comandos para el comando **groupadd**, y sustituya *group-name* por el nombre del grupo.

Ejemplo 6.2. Añadir un nuevo grupo

Para añadir el grupo **sysadmins** con el ID de grupo **5000**, utilice:

```
# groupadd -g 5000 sysadmins
```

Pasos de verificación

- Para comprobar que el nuevo grupo se ha añadido, utilice la utilidad **tail**.

```
# tail /etc/group
```

La salida devuelve:

```
sysadmins:x:5000:
```

Recursos adicionales

- **groupadd** página de manual

6.3. AÑADIR UN USUARIO A UN GRUPO DESDE LA LÍNEA DE COMANDOS

Esta sección describe cómo utilizar la utilidad **usermod** para añadir un grupo a los grupos suplementarios del usuario.

Requisitos previos

- **Root** acceso

Procedimiento

- Para añadir un grupo a los grupos complementarios del usuario, utilice:

```
# usermod --append -G group-name username
```

Sustituye *group-name* por el nombre del grupo, y sustituye *username* por el nombre del usuario.

Ejemplo 6.3. Añadir un usuario a un grupo

Para añadir el usuario **sysadmin** al grupo **system-administrators**, utilice:

```
# usermod --append -G system-administrators sysadmin
```

Pasos de verificación

- Para verificar que los nuevos grupos se añaden a los grupos suplementarios del usuario **sysadmin**, utilice:

```
# grupos sysadmin
```

La salida devuelve:

```
sysadmin: sysadmin system-administrators
```

6.4. CREACIÓN DE UN DIRECTORIO DE GRUPO

En la configuración del sistema UPG, se puede aplicar el bit *set-group identification permission* (**setgid**) a un directorio. El bit **setgid** simplifica la gestión de los proyectos de grupo que comparten un directorio. Cuando se aplica el bit **setgid** a un directorio, los archivos creados dentro de ese directorio se asignan automáticamente a un grupo que posee el directorio. Cualquier usuario que tenga permiso de escritura y ejecución dentro de este grupo puede ahora crear, modificar y eliminar archivos en el directorio.

La siguiente sección describe cómo crear directorios de grupo.

Requisitos previos

- **Root** acceso

Procedimiento

1. Crea un directorio:

```
# mkdir directory-name
```

Sustituya *directory-name* por el nombre del directorio.

2. Crea un grupo:

```
# groupadd group-name
```

Sustituya *group-name* por el nombre del grupo.

3. Añade usuarios al grupo:

```
# usermod --append -G group-name username
```

Sustituye *group-name* por el nombre del grupo, y sustituye[role=" *abstract"]e _username* por el nombre del usuario.

4. Asociar la propiedad del usuario y del grupo del directorio con el grupo *group-name*:

```
# chown group-name directory-name
```

Sustituye *group-name* por el nombre del grupo, y sustituye *directory-name* por el nombre del directorio.

5. Establezca los permisos de escritura para permitir a los usuarios crear y modificar archivos y directorios y establezca el bit **setgid** para que este permiso se aplique dentro del directorio *directory-name*:

```
# chmod g rwxs directory-name
```

Sustituya *directory-name* por el nombre del directorio.

Ahora todos los miembros del ***group-name*** grupo pueden crear y editar archivos en el directorio ***directory-name*** directorio. Los archivos recién creados conservan la propiedad del grupo ***group-name*** grupo.

Pasos de verificación

- Para verificar la corrección de los permisos establecidos, utilice:

```
# ls -ld directory-name
```

Sustituya *directory-name* por el nombre del directorio.

La salida devuelve:

```
drwxrwsr-x. 2 root group-name 6 Nov 25 08:45 directory-name
```

CAPÍTULO 7. ELIMINACIÓN DE UN USUARIO DE UN GRUPO MEDIANTE LA LÍNEA DE COMANDOS

Puedes eliminar un usuario de un grupo primario o complementario anulando los grupos a los que pertenece el usuario con un nuevo conjunto de grupos que no contenga el grupo del que quieres eliminar al usuario.

7.1. ANULACIÓN DEL GRUPO PRINCIPAL DE UN USUARIO

Esta sección describe cómo utilizar la utilidad **usermod** para anular el grupo primario del usuario.

Requisitos previos

- **Root** acceso

Procedimiento

- Para anular el grupo primario del usuario, utilice:

```
# usermod -g group-name username
```

Sustituye *group-name* por el nombre del grupo, y sustituye *username* por el nombre del usuario.

Ejemplo 7.1. Cambiar el grupo principal de un usuario

Si el usuario **sarah** pertenece a los grupos primarios **sarah1**, y quiere cambiar el grupo primario del usuario a **sarah2**, utilice:

```
# usermod -g sarah2 sarah
```

Pasos de verificación

- Para verificar que el grupo primario del usuario está anulado, utilice:

```
# grupos sarah
```

La salida devuelve:

```
sarah : sarah2
```

7.2. ANULACIÓN DE LOS GRUPOS COMPLEMENTARIOS DE UN USUARIO

Esta sección describe cómo utilizar la utilidad **usermod** para anular los grupos suplementarios del usuario.

Requisitos previos

- **Root** acceso

Procedimiento

- Para anular los grupos complementarios del usuario, utilice:

```
# usermod -G group-name username
```

Sustituye *group-name* por el nombre del grupo, y sustituye *username* por el nombre del usuario.

Ejemplo 7.2. Cambiar el grupo complementario de un usuario

Si el usuario **sarah** pertenece al grupo **system-administrator** y al grupo **developer** y quieres eliminar al usuario **sarah** del grupo **system-administrator**, puedes hacerlo sustituyendo la antigua lista de grupos por una nueva. Para ello, utiliza:

```
# usermod -G developer sarah
```

Pasos de verificación

- Para comprobar que los grupos complementarios del usuario están anulados, utilice:

```
# grupos sarah
```

La salida devuelve:

```
sarah : desarrollador de sarah
```

CAPÍTULO 8. CONCEDER ACCESO SUDO A UN USUARIO

Los administradores del sistema pueden conceder acceso a **sudo** para permitir a los usuarios no root ejecutar comandos administrativos. El comando **sudo** proporciona a los usuarios acceso administrativo sin utilizar la contraseña del usuario **root**.

Cuando los usuarios necesitan realizar un comando administrativo, pueden preceder ese comando con **sudo**. El comando se ejecuta entonces como si fuera el usuario **root**.

Ten en cuenta las siguientes limitaciones:

- Sólo los usuarios que figuran en el archivo de configuración **/etc/sudoers** pueden utilizar el comando **sudo**.
- El comando se ejecuta en el shell del usuario, no en el shell **root**.

Requisitos previos

- **Root** acceso

Procedimiento

1. Abra el archivo **/etc/sudoers**.

```
# visudo
```

   El archivo **/etc/sudoers** define las políticas aplicadas por el comando **sudo**.

2. En el archivo **/etc/sudoers** busque las líneas que conceden acceso a **sudo** a los usuarios del grupo administrativo **wheel**.

```
## Allows people in group wheel to run all commands
%wheel        ALL=(ALL)       ALL
```

3. Asegúrese de que la línea que comienza con **%wheel** no tiene el carácter de comentario **#** antes.
4. Guarde los cambios y salga del editor.
5. Añada los usuarios a los que desea conceder acceso a **sudo** en el grupo administrativo **wheel**.

```
# usermod --append -G wheel username
```

   Sustituya *username* por el nombre del usuario.

   Ejemplo 8.1. Añadir un usuario al grupo de la rueda

   Para añadir el usuario **sarah** al grupo administrativo **wheel**, utilice:

```
# usermod --append -G wheel sarah
```

Pasos de verificación

- Para comprobar que el usuario está añadido al grupo administrativo **wheel**, utilice la utilidad **id**.

```
# id sarah
```

La salida devuelve:

```
uid=5000(sarah) gid=5000(sarah) groups=5000(sarah),10(wheel)
```

CAPÍTULO 9. CAMBIO Y RESTABLECIMIENTO DE LA CONTRASEÑA DE ROOT

Si la contraseña de root existente ya no es satisfactoria o se ha olvidado, puede cambiarla o restablecerla tanto como usuario de **root** como como usuario no root.

9.1. CAMBIAR LA CONTRASEÑA DE ROOT COMO USUARIO ROOT

Esta sección describe cómo utilizar el comando **passwd** para cambiar la contraseña de **root** como usuario de **root**.

Requisitos previos

- **Root** acceso

Procedimiento

- Para cambiar la contraseña de **root**, utilice:

```
# passwd
```

  Se le pedirá que introduzca su contraseña actual antes de poder cambiarla.

9.2. CAMBIAR O RESTABLECER LA CONTRASEÑA DE ROOT OLVIDADA COMO USUARIO NO ROOT

Esta sección describe cómo utilizar el comando **passwd** para cambiar o restablecer la contraseña olvidada de **root** como usuario no root.

Requisitos previos

- Puede iniciar la sesión como usuario no root.
- Usted es miembro del grupo administrativo **wheel**.

Procedimiento

- Para cambiar o restablecer la contraseña de **root** como usuario no root que pertenece al grupo **wheel**, utilice:

```
$ sudo passwd root
```

  Se le pedirá que introduzca su contraseña actual, que no es de root, antes de poder cambiar la contraseña de **root**.

9.3. RESTABLECER LA CONTRASEÑA DE ROOT EN EL ARRANQUE

Si no puede iniciar sesión como usuario no root o no pertenece al grupo administrativo **wheel**, puede restablecer la contraseña de root en el arranque cambiando a un entorno especializado **chroot jail**.

Procedimiento

1. Reinicie el sistema y, en la pantalla de arranque de GRUB 2, pulse la tecla **e** para interrumpir el proceso de arranque.
   Aparecen los parámetros de arranque del kernel.

```
load_video
set gfx_payload=keep
insmod gzio
linux ($root)/vmlinuz-4.18.0-80.e18.x86_64 root=/dev/mapper/rhel-root ro crash\
kernel=auto resume=/dev/mapper/rhel-swap rd.lvm.lv/swap rhgb quiet
initrd ($root)/initramfs-4.18.0-80.e18.x86_64.img $tuned_initrd
```

2. Vaya al final de la línea que comienza con **linux**.

```
linux ($root)/vmlinuz-4.18.0-80.e18.x86_64 root=/dev/mapper/rhel-root ro crash\
kernel=auto resume=/dev/mapper/rhel-swap rd.lvm.lv/swap rhgb quiet
```

   Pulse **Ctrl e** para saltar al final de la línea.

3. Añada **rd.break** al final de la línea que comienza con **linux**.

```
linux ($root)/vmlinuz-4.18.0-80.e18.x86_64 root=/dev/mapper/rhel-root ro crash\
kernel=auto resume=/dev/mapper/rhel-swap rd.lvm.lv/swap rhgb quiet rd.break
```

4. Pulse **Ctrl x** para iniciar el sistema con los parámetros modificados.
   Aparece la indicación **switch_root**.

5. Volver a montar el sistema de archivos como escribible:

```
mount -o remount,rw /sysroot
```

   El sistema de archivos está montado como de sólo lectura en el directorio /**sysroot**. Volver a montar el sistema de archivos como de escritura permite cambiar la contraseña.

6. Entre en el entorno **chroot**:

```
chroot /sysroot
```

   Aparece la indicación **sh-4.4#**.

7. Restablece la contraseña de **root**:

```
passwd
```

   Siga las instrucciones mostradas por la línea de comandos para finalizar el cambio de la contraseña de **root**.

8. Habilitar el proceso de reetiquetado de SELinux en el siguiente arranque del sistema:

```
tocar /.autorelabel
```

9. Salga del entorno **chroot**:

```
salir
```

10. Salga de la página **switch_root**:

```
salir
```

11. Espere hasta que el proceso de reetiquetado de SELinux haya terminado. Tenga en cuenta que reetiquetar un disco grande puede llevar mucho tiempo. El sistema se reinicia automáticamente cuando termina el proceso.

Pasos de verificación

1. Para comprobar que la contraseña de **root** se ha modificado correctamente, inicie sesión como usuario normal y abra el Terminal.
2. Ejecute el shell interactivo como root:

```
$ su
```

3. Introduzca su nueva contraseña en **root**.
4. Imprime el nombre de usuario asociado a la ID de usuario efectiva actual:

```
whoami
```

La salida devuelve:

```
raíz
```

CAPÍTULO 10. GESTIÓN DE LOS PERMISOS DE LOS ARCHIVOS

10.1. INTRODUCCIÓN A LOS PERMISOS DE LOS ARCHIVOS

Cada archivo o directorio tiene tres niveles de propiedad:

- Usuario propietario (**u**).
- Propietario del grupo (**g**).
- Otros (**o**).

A cada nivel de propiedad se le pueden asignar los siguientes permisos:

- Leer (**r**).
- Escribe (**w**).
- Ejecutar (**x**).

Tenga en cuenta que el permiso de ejecución para un archivo le permite ejecutar ese archivo. El permiso de ejecución para un directorio le permite acceder al contenido del directorio, pero no ejecutarlo.

Cuando se crea un nuevo archivo o directorio, se le asigna automáticamente el conjunto de permisos por defecto. El permiso por defecto para un archivo o directorio se basa en dos factores:

- Permiso de base.
- El *user file-creation mode mask* (**umask**).

10.1.1. Permisos de base

Cada vez que se crea un nuevo archivo o directorio, se le asigna automáticamente un permiso base.

Los permisos base de un archivo o directorio pueden expresarse en valores *symbolic* o *octal*.

Permission	Symbolic value	Octal value
No hay permiso	---	0
Ejecutar	--x	1
Escriba	-w-	2
Escribir y ejecutar	-wx	3
Leer	r--	4
Leer y ejecutar	r-x	5

Leer y escribir	rw-	6
Leer, escribir, ejecutar	rwx	7

El permiso base para un directorio es **777** (**drwxrwxrwx**), que concede a todo el mundo los permisos de lectura, escritura y ejecución. Esto significa que el propietario del directorio, el grupo y otros pueden listar el contenido del directorio, crear, borrar y editar elementos dentro del directorio, y descender en él.

Tenga en cuenta que los archivos individuales dentro de un directorio pueden tener su propio permiso que podría impedirle editarlos, a pesar de tener acceso ilimitado al directorio.

El permiso base para un archivo es **666** (**-rw-rw-rw-**), que concede a todo el mundo los permisos de lectura y escritura. Esto significa que el propietario del archivo, el grupo y otros pueden leer y editar el archivo.

Ejemplo 1

Si un archivo tiene los siguientes permisos:

```
$ ls -l
-rwxrw----. 1 sysadmins sysadmins 2 Mar 2 08:43 file
```

- **-** indica que es un archivo.
- **rwx** indica que el propietario del archivo tiene permisos para leer, escribir y ejecutar el archivo.
- **rw-** indica que el grupo tiene permisos para leer y escribir, pero no para ejecutar el archivo.
- **---** indica que otros usuarios no tienen permiso para leer, escribir o ejecutar el archivo.
- **.** indica que el contexto de seguridad de SELinux está establecido para el archivo.

Ejemplo 2

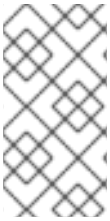
Si un directorio tiene los siguientes permisos:

```
$ ls -dl directory
drwxr-----. 1 sysadmins sysadmins 2 Mar 2 08:43 directory
```

- **d** indica que es un directorio.
- **rwx** indica que el propietario del directorio tiene los permisos para leer, escribir y acceder al contenido del directorio.
  Como propietario de un directorio, puede enumerar los elementos (archivos, subdirectorios) dentro del directorio, acceder al contenido de esos elementos y modificarlos.
- **r--** indica que el grupo tiene permisos para leer, pero no para escribir o acceder al contenido del directorio.
  Como miembro del grupo propietario del directorio, puede listar los elementos del directorio. No puede acceder a la información de los elementos dentro del directorio ni modificarlos.
- **---** indica que otros usuarios no tienen permiso para leer, escribir o acceder al contenido del directorio.

Como alguien que no es propietario de un usuario, o como propietario de un grupo del directorio, no puede listar los elementos dentro del directorio, acceder a la información sobre esos elementos o modificarlos.

- **.** indica que el contexto de seguridad SELinux está establecido para el directorio.



NOTA

El permiso base que se asigna automáticamente a un archivo o directorio es **not** el permiso por defecto con el que termina el archivo o directorio. Cuando se crea un archivo o directorio, el permiso base es alterado por el *umask*. La combinación del permiso base y el *umask* crea el permiso por defecto para los archivos y directorios.

10.1.2. Máscara del modo de creación de archivos del usuario

La *umask* es una variable que elimina automáticamente los permisos del valor de permiso base cada vez que se crea un archivo o directorio para aumentar la seguridad general de un sistema linux.

El *umask* puede expresarse en *symbolic* o *octal*.

Permission	Symbolic value	Octal value
Leer, escribir y ejecutar	rwx	0
Leer y escribir	rw-	1
Leer y ejecutar	r-x	2
Leer	r--	3
Escribir y ejecutar	-wx	4
Escriba	-w-	5
Ejecutar	--x	6
No hay permisos	---	7

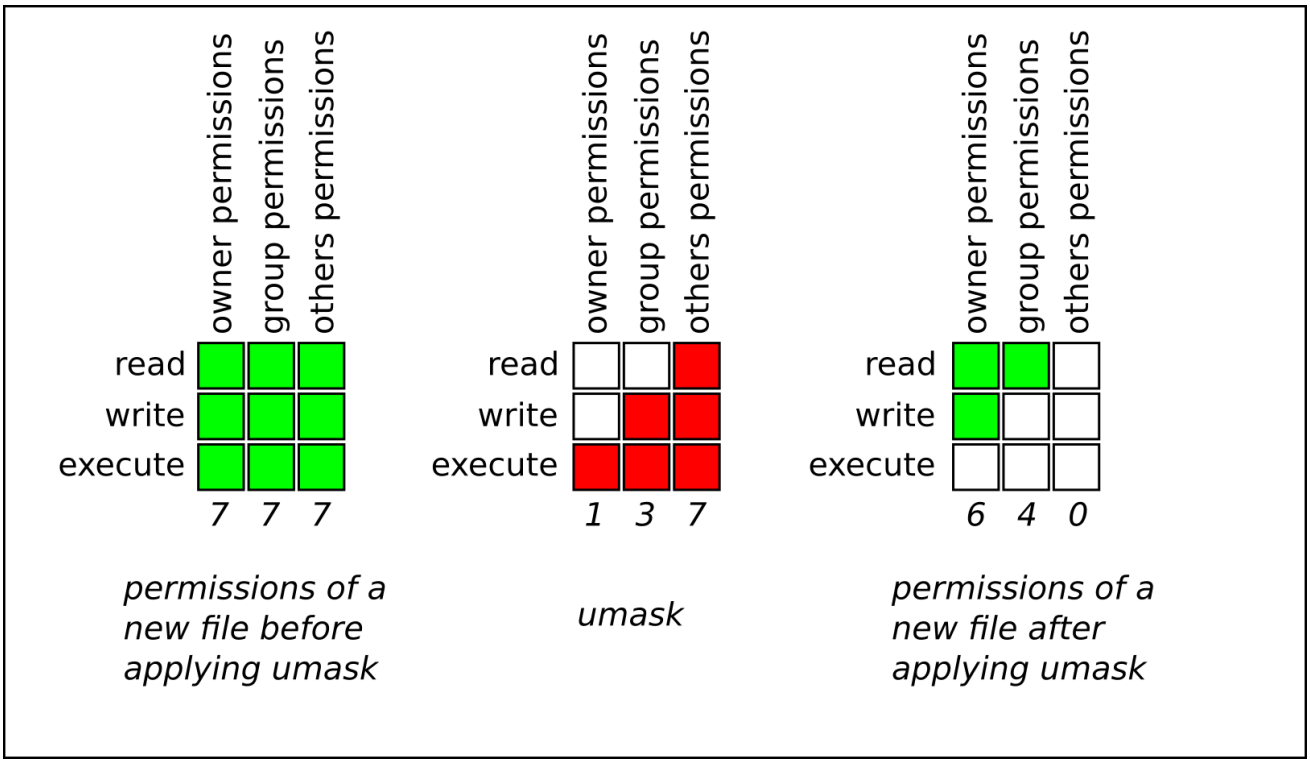
El valor por defecto de *umask* para un usuario estándar es **0002**. El valor por defecto de *umask* para un usuario **root** es **0022**.

El primer dígito de *umask* representa los permisos especiales (sticky bit,). Los tres últimos dígitos de *umask* representan los permisos que se quitan al usuario propietario (**u**), al propietario del grupo (**g**), y a otros (**o**) respectivamente.

Ejemplo

El siguiente ejemplo ilustra cómo el *umask* con un valor octal de **0137** se aplica al archivo con el permiso base de **777**, para crear el archivo con el permiso por defecto de **640**.

Figura 10.1. Aplicación de la umask al crear un archivo



10.1.3. Permisos por defecto

El permiso por defecto para un nuevo archivo o directorio se determina aplicando el *umask* al permiso base.

Ejemplo 1

Cuando un **standard user** crea un nuevo **directory**, el *umask* se establece en **002** (**rwxrwxr-x**), y el permiso base para un directorio se establece en **777** (**rwxrwxrwx**). Esto hace que el permiso por defecto sea **775** (**drwxrwxr-x**).

	Symbolic value	Octal value
Base permission	rwxrwxrwx	777
Umask	rwxrwxr-x	002
Default permission	rwxrwxr-x	775

Esto significa que el propietario del directorio y el grupo pueden listar el contenido del directorio, crear, borrar y editar elementos dentro del directorio, y descender en él. Los demás usuarios sólo pueden listar el contenido del directorio y descender a él.

Ejemplo 2

Cuando un **standard user** crea un nuevo **file**, el *umask* se establece en **002** (**rwxrwxr-x**), y el permiso base para un archivo se establece en **666** (**rw-rw-rw-**). Esto hace que el permiso por defecto sea **664** (**-rw-rw-r--**).

	Symbolic value	Octal value
Base permission	rw-rw-rw-	666
Umask	rwxrwxr-x	002
Default permission	rw-rw-r--	664

Esto significa que el propietario del archivo y el grupo pueden leer y editar el archivo, mientras que los demás usuarios sólo pueden leerlo.

Ejemplo 3

Cuando un **root user** crea un nuevo **directory**, el *umask* se establece en **022** (**rwxr-xr-x**), y el permiso base para un directorio se establece en **777** (**rwxrwxrwx**). Esto hace que el permiso por defecto sea **755** (**rwxr-xr-x**).

	Symbolic value	Octal value
Base permission	rwxrwxrwx	777
Umask	rwxr-xr-x	022
Default permission	rwxr-xr-x	755

Esto significa que el propietario del directorio puede listar el contenido del mismo, crear, borrar y editar elementos dentro del directorio, y descender en él. El grupo y los demás sólo pueden listar el contenido del directorio y descender a él.

Ejemplo 4

Cuando un **root user** crea un nuevo **file**, el *umask* se establece en **022** (**rwxr-xr-x**), y el permiso base para un archivo se establece en **666** (**rw-rw-rw-**). Esto hace que el permiso por defecto sea **644** (**-rw-r—r--**).

	Symbolic value	Octal value
Base permission	rw-rw-rw-	666
Umask	rwxr-xr-x	022
Default permission	rw-r-r--	644

Esto significa que el propietario del archivo puede leer y editar el archivo, mientras que el grupo y otros sólo pueden leer el archivo.

NOTA

Por razones de seguridad, los archivos normales no pueden tener permisos de ejecución por defecto, incluso si el *umask* está configurado como **000** (**rwxrwxrwx**). Sin embargo, se pueden crear directorios con permisos de ejecución.

10.2. VISUALIZACIÓN DE LOS PERMISOS DE LOS ARCHIVOS

La siguiente sección describe cómo utilizar el comando **ls** para mostrar los permisos de los directorios, archivos y archivos dentro de los directorios.

Procedimiento

- Para ver los permisos de un directorio en particular, utilice:

```
$ ls -dl directory-name
```

  Sustituya *directory-name* por el nombre del directorio.

- Para ver los permisos de todos los archivos de un determinado directorio, utilice

```
$ ls -l directory-name
```

  Sustituya *directory-name* por el nombre del directorio.

- Para ver los permisos de un archivo en particular, utilice:

```
$ ls -l file-name
```

  Sustituya *file-name* por el nombre del archivo.

Información adicional

- Consulte la página de manual **ls** para obtener más detalles.

10.3. CAMBIAR LOS PERMISOS DE LOS ARCHIVOS

La siguiente sección describe cómo:

- Cambiar los permisos de los archivos utilizando valores simbólicos.
- Cambiar los permisos de los archivos utilizando valores octales.

10.3.1. Modificación de los permisos de los archivos mediante valores simbólicos

Puede asignar los siguientes permisos:

- Leer (**r**).
- Escribe (**w**).
- Ejecutar (**x**).

Los permisos se pueden asignar a:

- Usuario propietario (**u**).
- Propietario del grupo (**g**).
- Otros (**o**).
- Todos (**a**).

Para añadir o quitar los permisos puede utilizar los siguientes signos:

- para añadir los permisos sobre los ya existentes.
- **-** para quitar los permisos del permiso existente.
- **=** para omitir los permisos existentes y definir explícitamente los nuevos.

La siguiente sección describe cómo establecer y eliminar los permisos de los archivos utilizando los valores simbólicos.

Procedimiento

- Para cambiar los permisos de un archivo o directorio existente, utilice:

```
$ chmod u=symbolic_value,g symbolic_value,o-symbolic_value file-name
```

Sustituya *file-name* por el nombre del archivo o directorio, y sustituya *symbolic_value* para el usuario, los grupos y otros por los valores simbólicos correspondientes. Consulte Sección 10.1.1, “Permisos de base” para obtener más detalles.

Ejemplo

Para cambiar los permisos del archivo **my-file.txt** de **664** (**-rw-rw-r--**) a **740** (**-rwx-r---**), utilice:

```
$ chmod u x,g-w,o= mi-archivo.txt
```

Tenga en cuenta que cualquier permiso que no se especifique después del signo de igualdad (**=**) queda automáticamente prohibido.

- Para establecer los mismos permisos para el usuario, el grupo y otros, utilice:

```
$ chmod a=symbolic_value file-name
```

Sustituya *file-name* por el nombre del archivo o directorio, y sustituya *symbolic_value* por un valor simbólico. Consulte Sección 10.1.1, “Permisos de base” para obtener más detalles.

Ejemplo

Para establecer el permiso de **my-file.txt** a **777** (**-rwxrwxrwx** o **drwxrwxrwx**), utilice:

```
$ chmod a=rwx mi-archivo
```

- Para cambiar los permisos de un directorio y de todos sus subdirectorios, añada la opción **-R**:

```
$ chmod -R symbolic_value directory-name
```

Sustituya *directory-name* por el nombre del directorio y sustituya *symbolic_value* por un valor simbólico. Consulte Sección 10.1.1, "Permisos de base" para obtener más detalles.

Ejemplo

Para cambiar los permisos de /**my-directory**/ y todos sus subdirectorios de **775** (**drwxrwxr-x**) a **740** (**drwx-r---**), utilice:

```
$ chmod -R g-wx,o= /mi-directorio
```

10.3.2. Modificación de los permisos de los archivos mediante valores octales

La siguiente sección describe cómo utilizar el comando **chmod** para cambiar los permisos de un archivo o directorio.

Procedimiento

- Para cambiar los permisos de un archivo o directorio existente, utilice:

  ```
  $ chmod octal_value file-name
  ```

  Sustituya *file-name* por el nombre del archivo o directorio, y sustituya *octal_value* por un valor octal. Consulte Sección 10.1.1, "Permisos de base" para obtener más detalles.

10.4. VISUALIZACIÓN DE LA UMASK

La siguiente sección describe cómo:

- Muestra el valor octal actual de *umask*.
- Muestra el valor simbólico actual de *umask*.
- Mostrar el bash por defecto *umask*.

10.4.1. Mostrar el valor octal actual de la umask

En la siguiente sección se describe cómo utilizar el comando **umask** para mostrar el *umask* actual.

Procedimiento:

- Para mostrar el valor octal actual de la *umask* para un usuario estándar, utilice:

  ```
  $ umask
  ```

- Para mostrar el valor octal actual de la *umask* para un usuario de **root**, utilice:

  ```
  $ sudo umask
  ```

  O:

  ```
  # umask
  ```

10.4.2. Mostrar el valor simbólico actual de la umask

En la siguiente sección se describe cómo utilizar el comando **umask** para mostrar el *umask* actual.

Procedimiento

- Para mostrar el valor simbólico actual de *umask*, utilice:

```
$ umask -S
```

- Para mostrar el valor simbólico actual de la *umask* para un usuario de **root**, utilice:

```
$ sudo umask -S
```

O:

```
# umask -S
```

10.4.3. Visualización de la umask de bash por defecto

Hay una serie de conchas que puedes utilizar, como **bash**, **ksh**, **zsh** y **tcsh**.

Estos shells pueden comportarse como shells de inicio de sesión o no. El shell de inicio de sesión se suele invocar abriendo un terminal nativo o un GUI.

Para determinar si está ejecutando un comando en un shell de inicio de sesión o no, utilice el comando **echo $0**.

En **bash** shell, si la salida devuelve **bash**, se está ejecutando un comando en un shell que no es de acceso.

```
$ echo $0
bash
```

El valor por defecto de *umask* para el shell que no es de inicio de sesión se establece en el archivo de configuración /**etc**/**bashrc**.

Si la salida devuelve **-bash**, está ejecutando un comando en un shell de acceso.

```
# echo $0
-bash
```

La dirección *umask* por defecto para el shell de inicio de sesión se establece en el archivo de configuración /**etc**/**profile**.

Procedimiento

- Para mostrar la página web **bash** *umask* por defecto para el intérprete de comandos que no es de acceso, utilice:

```
$ grep umask /etc/bashrc
```

La salida devuelve:

```
# By default, we want umask to get set. This sets it for non-login shell.
    umask 002
    umask 022
```

- Para mostrar la dirección **bash** *umask* por defecto para el shell de inicio de sesión, utilice:

```
$ grep umask /etc/profile
```

La salida devuelve:

```
# By default, we want umask to get set. This sets it for login shell
    umask 002
    umask 022
```

10.5. ESTABLECER LA UMASK PARA LA SESIÓN DE SHELL ACTUAL

En la siguiente sección se describe cómo establecer la dirección *umask* para la sesión actual del shell:

- Utilización de valores simbólicos.
- Utilizando valores octales.

Tenga en cuenta que la dirección *umask* sólo es válida durante la sesión actual del shell y vuelve a la dirección *umask* por defecto una vez finalizada la sesión.

10.5.1. Establecer la umask utilizando valores simbólicos

En la siguiente sección se describe cómo configurar el *umask* con valores simbólicos.

Procedimiento

- Para establecer o eliminar los permisos de la sesión actual del shell, puede utilizar los signos menos (**-**), más ( ) e igual (**=**) en combinación con valores simbólicos.

```
$ umask -S u=symbolic_value,g symbolic_value,o-symbolic_value
```

Reemplazar *symbolic_value* para usuario, grupo y otros con valores simbólicos. Consulte Sección 10.1.2, “Máscara del modo de creación de archivos del usuario” para más detalles.

Ejemplo

Si tu actual *umask* está configurado como **113** (**u=rw-,g=rw-,o=r--**) y quieres configurarlo como **037** (**u=rwx,g=-r-,o=---**), utiliza:

```
$ umask -S u x,g-w,o=
```

Tenga en cuenta que cualquier permiso que no se especifique después del signo de igualdad (**=**) queda automáticamente prohibido.

- Para establecer los mismos permisos para el usuario, el grupo y otros, utilice:

```
$ umask a=symbolic_value
```

Sustituir *symbolic_value* por un valor simbólico. Consulte Sección 10.1.2, "Máscara del modo de creación de archivos del usuario" para obtener más detalles.

Ejemplo

Para ajustar el *umask* a **000** (**u=rwx,g=rwx,o=rwx**), utilice:

```
$ umask a=rwx
```

Tenga en cuenta que la dirección *umask* sólo es válida para la sesión actual del shell.

10.5.2. Establecer la umask utilizando valores octales

En la siguiente sección se describe cómo configurar el *umask* con valores octales.

Procedimiento

- Para establecer el *umask* para la sesión actual del shell utilizando valores octales, utilice:

```
$ umask octal_value
```

Sustituya *octal_value* por un valor octal. Consulte Sección 10.1.2, "Máscara del modo de creación de archivos del usuario" para obtener más detalles.

Tenga en cuenta que la dirección *umask* sólo es válida para la sesión actual del shell.

10.6. CAMBIAR LA UMASK POR DEFECTO

La siguiente sección describe cómo:

- Cambia el bash *umask* por defecto para el shell que no es de acceso.
- Cambia el bash *umask* por defecto para el shell de inicio de sesión.
- Cambiar el bash *umask* por defecto para un usuario específico.
- Establece los permisos por defecto para los directorios de inicio recién creados.

Requisitos previos

- **Root** acceso.

10.6.1. Cambio de la máscara de umask por defecto para el shell que no es de inicio de sesión

En la siguiente sección se describe cómo cambiar la dirección **bash** *umask* por defecto para los usuarios estándar.

Procedimiento

1. Como **root**, abra el archivo **/etc/bashrc** en un editor de su elección.
2. Modifique las siguientes secciones para establecer un nuevo bash por defecto *umask*:

```
if [ $UID -gt 199 ] && [ “id -gn” = “id -un” ]; then
  umask 002
else
  umask 022
fi
```

Sustituye el valor octal por defecto de *umask* (**002**) por otro valor octal. Consulte Sección 10.1.2, “Máscara del modo de creación de archivos del usuario” para obtener más detalles.

3. Guarde los cambios.

10.6.2. Cambio de la umask por defecto para el shell de inicio de sesión

La siguiente sección describe cómo cambiar la dirección de correo electrónico por defecto **bash** *umask* para el usuario **root**.

Procedimiento

1. Como **root**, abra el archivo **/etc/profile** en un editor de su elección.
2. Modifique las siguientes secciones para establecer un nuevo bash por defecto *umask*:

```
if [ $UID -gt 199 ] && [ “/usr/bin/id -gn” = “/usr/bin/id -un” ]; then
   umask 002
else
   umask 022
fi
```

Sustituye el valor octal por defecto de *umask* (**022**) por otro valor octal. Consulte Sección 10.1.2, “Máscara del modo de creación de archivos del usuario” para obtener más detalles.

3. Guarde los cambios.

10.6.3. Cambiar la umask por defecto para un usuario específico

La siguiente sección describe cómo cambiar la dirección *umask* por defecto para un usuario específico.

Procedimiento

- Ponga la línea que especifica el valor octal de la *umask* en el archivo **.bashrc** para el usuario particular.

```
$ echo 'umask octal_value' >> /home/username/.bashrc
```

Sustituya *octal_value* por un valor octal y sustituya *username* por el nombre del usuario. Consulte Sección 10.1.2, “Máscara del modo de creación de archivos del usuario” para obtener más detalles.

10.6.4. Establecer el UMASK por defecto para los directorios de inicio recién creados

La siguiente sección describe cómo cambiar los permisos que especifican el *UMASK* para los directorios personales de los usuarios recién creados.

Procedimiento

1. Como **root**, abra el archivo **/etc/login.defs** en un editor de su elección.
2. Modifique la siguiente sección para establecer un nuevo valor por defecto *UMASK*:

```
# The permission mask is initialized to this value. If not specified,
# the permission mask will be initialized to 022.
UMASK 077
```

   Sustituye el valor octal por defecto (**077**) por otro valor octal. Consulte Sección 10.1.2, “Máscara del modo de creación de archivos del usuario” para obtener más detalles.

3. Guarde los cambios.

10.7. LISTA DE CONTROL DE ACCESO

Tradicionalmente, cada archivo y directorio sólo puede tener un propietario de usuario y un propietario de grupo a la vez. Si quieres aplicar un conjunto más específico de permisos a un archivo o directorio (permitir que ciertos usuarios fuera del grupo tengan acceso a un archivo específico dentro de un directorio pero no a otros archivos) sin cambiar la propiedad y los permisos de un archivo o directorio, puedes utilizar las listas de control de acceso (ACL).

La siguiente sección describe cómo:

- Muestra la ACL actual.
- Establece la ACL.

10.7.1. Visualización de la ACL actual

La siguiente sección describe cómo mostrar la ACL actual.

Procedimiento

- Para mostrar la ACL actual de un archivo o directorio concreto, utilice:

```
$ getfacl file-name
```

  Sustituya *file-name* por el nombre del archivo o directorio.

10.7.2. Configuración de la ACL

La siguiente sección describe cómo configurar la ACL.

Requisitos previos

- **Root** acceso

Procedimiento

- Para establecer la ACL de un archivo o directorio, utilice:

```
# setfacl -m u:username:symbolic_value file-name
```

Sustituya *username* por el nombre del usuario, *symbolic_value* por un valor simbólico y *file-name* por el nombre del archivo o directorio. Para más información, consulte la página de manual **setfacl**.

Ejemplo

El siguiente ejemplo describe cómo modificar los permisos del archivo **group-project** propiedad del usuario **root** que pertenece al grupo **root** para que este archivo sea:

- No es ejecutable por nadie.
- El usuario **andrew** tiene el permiso **rw-**.
- El usuario **susan** tiene el permiso **---**.
- Otros usuarios tienen el permiso **r--**.

Procedimiento

```
# setfacl -m u:andrew:rw- group-project
# setfacl -m u:susan:--- group-project
```

Pasos de verificación

- Para verificar que el usuario **andrew** tiene el permiso **rw-**, el usuario **susan** tiene el permiso **---**, y otros usuarios tienen el permiso **r--**, utilice:

  ```
  $ getfacl grupo-proyecto
  ```

  La salida devuelve:

  ```
  # file: group-project
  # owner: root
  # group: root
  user:andrew:rw-
  user:susan:---
  group::r--
  mask::rw-
  other::r--
  ```

CAPÍTULO 11. USO DE LA SUITE CHRONY PARA CONFIGURAR NTP

11.1. INTRODUCCIÓN A LA CONFIGURACIÓN DE NTP CON CHRONY

La precisión de la hora es importante por varias razones en TI. En las redes, por ejemplo, se necesitan marcas de tiempo precisas en los paquetes y registros. En los sistemas Linux, el protocolo **NTP** está implementado por un demonio que se ejecuta en el espacio de usuario.

El demonio del espacio de usuario actualiza el reloj del sistema que se ejecuta en el núcleo. El reloj del sistema puede mantener la hora utilizando varias fuentes de reloj. Normalmente, se utiliza el *Time Stamp Counter* (**TSC**). El TSC es un registro de la CPU que cuenta el número de ciclos desde que se reinició por última vez. Es muy rápido, tiene una alta resolución y no hay interrupciones.

En Red Hat Enterprise Linux 8, el protocolo **NTP** es implementado por el demonio **chronyd**, disponible en los repositorios en el paquete **chrony**.

Estas secciones describen el uso del **chrony** suite.

11.2. INTRODUCCIÓN A CHRONY SUITE

chrony es una implementación de la página web **Network Time Protocol (NTP)**. Puede utilizar **chrony**:

- Para sincronizar el reloj del sistema con los servidores **NTP**
- Para sincronizar el reloj del sistema con un reloj de referencia, por ejemplo un receptor GPS
- Para sincronizar el reloj del sistema con una entrada de hora manual
- Como servidor **NTPv4(RFC 5905)** o peer para proporcionar un servicio de tiempo a otros ordenadores de la red

chrony tiene un buen rendimiento en una amplia gama de condiciones, incluidas las conexiones de red intermitentes, las redes muy congestionadas, los cambios de temperatura (los relojes de los ordenadores ordinarios son sensibles a la temperatura) y los sistemas que no funcionan de forma continua, o que se ejecutan en una máquina virtual.

La precisión típica entre dos máquinas sincronizadas a través de Internet es de unos pocos milisegundos, y para las máquinas en una LAN de decenas de microsegundos. La marca de tiempo por hardware o un reloj de referencia por hardware pueden mejorar la precisión entre dos máquinas sincronizadas a un nivel de sub-microsegundos.

chrony consiste en **chronyd**, un demonio que se ejecuta en el espacio de usuario, y **chronyc**un programa de línea de comandos que puede utilizarse para supervisar el rendimiento de **chronyd** y para cambiar varios parámetros de funcionamiento cuando se está ejecutando.

El demonio **chrony** daemon, **chronyd**, puede ser supervisado y controlado por la utilidad de línea de comandos **chronyc**. Esta utilidad proporciona una línea de comandos que permite introducir una serie de órdenes para consultar el estado actual de **chronyd** y realizar cambios en su configuración. Por defecto, **chronyd** sólo acepta órdenes de una instancia local de **chronyc**pero se puede configurar para que acepte comandos de monitorización también desde hosts remotos. El acceso remoto debe ser restringido.

11.2.1. Uso de chronyc para controlar chronyd

Para realizar cambios en la instancia local de **chronyd** utilizando la utilidad de línea de comandos **chronyc** en modo interactivo, introduzca el siguiente comando como **root**:

```
# chronyc
```

chronyc debe ejecutarse como **root** si se van a utilizar algunos de los comandos restringidos.

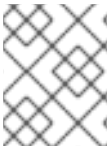
El comando **chronyc** el símbolo del sistema se mostrará de la siguiente manera:

```
chronyc>
```

Puedes teclear **help** para listar todos los comandos.

La utilidad también puede ser invocada en modo de comando no interactivo si se llama junto con un comando de la siguiente manera:

chronyc ***command***



NOTA

Los cambios realizados con **chronyc** no son permanentes, se perderán tras un reinicio de **chronyd**. Para los cambios permanentes, modifique **/etc/chrony.conf**.

11.3. DIFERENCIAS ENTRE CHRONY Y NTP

Network Time Protocol (NTP) tiene dos implementaciones diferentes con una funcionalidad básica similar - **ntp** y **chrony**.

Tanto **ntp** como **chrony** pueden funcionar como clientes de **NTP** para sincronizar el reloj del sistema con los servidores de **NTP** y pueden funcionar como servidores de **NTP** para otros ordenadores de la red. Cada implementación tiene algunas características únicas. Para comparar **ntp** y **chrony**ver Comparación de implementaciones NTP .

La configuración específica de un cliente **NTP** es idéntica en la mayoría de los casos. Los servidores **NTP** se especifican con la directiva **server**. Se puede especificar un conjunto de servidores con la directiva **pool**.

La configuración específica de un servidor **NTP** difiere en cómo se controla el acceso del cliente. Por defecto, **ntpd** responde a las peticiones de los clientes desde cualquier dirección. El acceso se puede restringir con la directiva **restrict**, pero no es posible deshabilitar el acceso completamente si **ntpd** utiliza cualquier servidor como cliente. **chronyd** no permite ningún acceso por defecto y funciona sólo como cliente de **NTP**. Para hacer que **chrony** funcione como un servidor **NTP**, es necesario especificar algunas direcciones dentro de la directiva **allow**.

ntpd y **chronyd** difieren también en el comportamiento por defecto con respecto a las correcciones del reloj del sistema. **ntpd** corrige el reloj por pasos cuando el desfase es mayor de 128 milisegundos. Si el desfase es mayor de 1000 segundos, **ntpd** sale a no ser que sea la primera corrección del reloj y se inicie **ntpd** con la opción **-g**. **chronyd** no corrige el reloj por pasos por defecto, pero el archivo **chrony.conf** por defecto proporcionado en el paquete **chrony** permite los pasos en las tres primeras actualizaciones del reloj. Después de eso, todas las correcciones se hacen lentamente acelerando o ralentizando el reloj. El comando **chronyc makestep** puede ser emitido para forzar a **chronyd** a escalar el reloj en cualquier momento.

11.4. MIGRACIÓN A LA CRONOLOGÍA

En Red Hat Enterprise Linux 7, los usuarios podían elegir entre **ntp** y **chrony** para asegurar la exactitud de la hora. Para las diferencias entre **ntp** y **chrony** **ntpd** y **chronyd**, consulte las diferencias entre ntpd y chronyd.

En Red Hat Enterprise Linux 8, **ntp** ya no está soportado **chrony** está activado por defecto. Por esta razón, podría necesitar migrar de **ntp** a **chrony**.

La migración de **ntp** a **chrony** es sencillo en la mayoría de los casos. Los nombres correspondientes de los programas, archivos de configuración y servicios son:

Tabla 11.1. Nombres correspondientes de los programas, archivos de configuración y servicios al migrar de ntp a chrony

nombre ntp	nombre de la crono
/etc/ntp.conf	/etc/chrony.conf
/etc/ntp/keys	/etc/chrony.keys
ntpd	chronyd
ntpq	chronyc
ntpd.service	cronoservicio
ntp-wait.service	chrony-wait.service

El **ntpdate** y **sntp** que se incluyen en la distribución **ntp**, pueden sustituirse por **chronyd** utilizando la opción **-q** o la opción **-t**. La configuración puede especificarse en la línea de comandos para evitar la lectura de **/etc/chrony.conf**. Por ejemplo, en lugar de ejecutar **ntpdate ntp.example.com**, **chronyd** podría iniciarse como:

```
# chronyd -q 'server ntp.example.com iburst'
2018-05-18T12:37:43Z chronyd version 3.3 starting (+CMDMON +NTP +REFCLOCK +RTC
+PRIVDROP +SCFILTER +SIGND +ASYNCDNS +SECHASH +IPV6 +DEBUG)
2018-05-18T12:37:43Z Initial frequency -2.630 ppm
2018-05-18T12:37:48Z System clock wrong by 0.003159 seconds (step)
2018-05-18T12:37:48Z chronyd exiting
```

La utilidad **ntpstat** utilidad, que antes estaba incluida en el paquete **ntp** y sólo soportaba **ntpd**, ahora soporta tanto **ntpd** como **chronyd**. Está disponible en el paquete **ntpstat**.

11.4.1. Guión de migración

En la documentación del paquete **chrony** (**/usr/share/doc/chrony**) se incluye un script de Python llamado **ntp2chrony.py**. El script convierte automáticamente una configuración existente de **ntp** a **chrony**. Soporta las directivas y opciones más comunes del archivo **ntp.conf**. Las líneas que se ignoran en la conversión se incluyen como comentarios en el archivo **chrony.conf** generado para su revisión. Las claves que se especifican en el archivo de claves **ntp**, pero que no están marcadas como claves de confianza en **ntp.conf** se incluyen en el archivo generado **chrony.keys** como comentarios.

Por defecto, el script no sobrescribe ningún archivo. Si **/etc/chrony.conf** o **/etc/chrony.keys** ya existen, se puede utilizar la opción **-b** para renombrar el archivo como copia de seguridad. El script admite otras opciones. La opción **--help** imprime todas las opciones soportadas.

Un ejemplo de invocación del script con la dirección **ntp.conf** por defecto proporcionada en el paquete **ntp** es:

```
# python3 /usr/share/doc/chrony/ntp2chrony.py -b -v
Reading /etc/ntp.conf
Reading /etc/ntp/crypto/pw
Reading /etc/ntp/keys
Writing /etc/chrony.conf
Writing /etc/chrony.keys
```

La única directiva que se ignora en este caso es **disable monitor**, que tiene un equivalente en la directiva **noclientlog**, pero que se incluyó en la directiva por defecto **ntp.conf** sólo para mitigar un ataque de amplificación.

El archivo **chrony.conf** generado suele incluir una serie de directivas **allow** correspondientes a las líneas de restricción de **ntp.conf**. Si no desea ejecutar **chronyd** como un servidor **NTP**, elimine todas las directivas **allow** de **chrony.conf**.

11.4.2. Función Timesync

Tenga en cuenta que el uso del rol timesync en su sistema Red Hat Enterprise Linux 7 facilita la migración a **chrony**porque puede utilizar el mismo playbook en todas las versiones de RHEL, empezando por RHEL 6, independientemente de si el sistema utiliza **ntp** o **chrony** para implementar el protocolo NTP.

Recursos adicionales

- Para una referencia detallada sobre las variables de rol de **timesync**, instale el paquete **rhel-system-roles**, y vea los archivos **README.md** o **README.html** en el directorio **/usr/share/doc/rhel-system-roles/timesync**.
- Para más información sobre los roles de sistema de RHEL, consulte Introducción a los roles de sistema de RHEL.

11.5. CONFIGURACIÓN DE LA CRONÍA

El archivo de configuración por defecto para **chronyd** es **/etc/chrony.conf**. La opción **-f** puede utilizarse para especificar una ruta de archivo de configuración alternativa. Consulte la página de manual **chrony.conf(5)** para conocer otras opciones. Para una lista completa de las directivas que se pueden utilizar, consulte El archivo de configuración chronyd .

A continuación se muestra una selección de opciones de configuración de **chronyd**:

Comentarios

Los comentarios deben ir precedidos de #, %, ; o !

permitir

Opcionalmente, especifique un host, una subred o una red desde la que permitir las conexiones de **NTP** a una máquina que actúe como servidor de **NTP**. El valor por defecto es no permitir conexiones. Ejemplos:

```
permitir 192.0.2.0/24
```

Utilice este comando para conceder acceso a una red específica.

```
allow 2001:0db8:85a3::8a2e:0370:7334
```

Utilice este comando para conceder acceso a un **IPv6**.

El puerto UDP número 123 debe estar abierto en el firewall para permitir el acceso del cliente:

```
# firewall-cmd --zone=public --add-port=123/udp
```

Si quiere abrir el puerto 123 de forma permanente, utilice la opción **--permanent**:

```
# firewall-cmd --permanent --zone=public --add-port=123/udp
```

cmdallow

Es similar a la directiva **allow** (véase la sección **allow**), excepto que permite el acceso de control (en lugar de **NTP** acceso de cliente) a una subred o host en particular. (Por "acceso de control" se entiende que **chronyc** puede ejecutarse en esos hosts y conectarse con éxito a **chronyd** en este equipo) La sintaxis es idéntica. También existe una directiva **cmddeny all** con un comportamiento similar a la directiva **cmdallow all**.

dumpdir

Ruta de acceso al directorio para guardar el historial de mediciones en los reinicios de **chronyd** (suponiendo que no se realicen cambios en el comportamiento del reloj del sistema mientras no se esté ejecutando). Si se va a utilizar esta capacidad (mediante el comando **dumponexit** en el archivo de configuración, o el comando **dump** en **chronyc**), el comando **dumpdir** debe utilizarse para definir el directorio donde se guardan los historiales de medición.

dumponexit

Si este comando está presente, indica que **chronyd** debe guardar el historial de mediciones para cada una de sus fuentes de tiempo registradas cada vez que el programa salga. (Véase el comando **dumpdir** más arriba).

hwtimestamp

La directiva **hwtimestamp** permite el marcado de tiempo por hardware para una sincronización extremadamente precisa. Para más detalles, consulte la página del manual **chrony.conf(5)**.

local

La palabra clave **local** se utiliza para permitir que **chronyd** aparezca sincronizado con el tiempo real desde el punto de vista de los clientes que lo sondean, incluso si no tiene una fuente de sincronización actual. Esta opción se utiliza normalmente en el ordenador "maestro" en una red aislada, donde se requiere que varios ordenadores se sincronicen entre sí, y el "maestro" se mantiene en línea con el tiempo real mediante la entrada manual.
Un ejemplo del comando es:

```
estrato local 10
```

Un valor grande de 10 indica que el reloj está a tantos saltos de un reloj de referencia que su hora no es fiable. Si el ordenador tiene alguna vez acceso a otro ordenador que, en última instancia, esté sincronizado con un reloj de referencia, es casi seguro que estará en un estrato inferior a 10. Por lo tanto, la elección de un valor alto como 10 para el comando **local** evita que la hora propia de la máquina se confunda con la hora real, si alguna vez se filtra a los clientes que tienen visibilidad de los servidores reales.

registro

El comando **log** indica que se debe registrar cierta información. Acepta las siguientes opciones:

medidas

Esta opción registra las mediciones en bruto de **NTP** y la información relacionada en un archivo llamado **measurements.log**.

estadísticas

Esta opción registra información sobre el procesamiento de la regresión en un archivo llamado **statistics.log**.

rastreando

Esta opción registra los cambios en la estimación de la tasa de ganancia o pérdida del sistema, y cualquier giro realizado, en un archivo llamado **tracking.log**.

rtc

Esta opción registra información sobre el reloj en tiempo real del sistema.

refclocks

Esta opción registra las mediciones del reloj de referencia crudas y filtradas en un archivo llamado **refclocks.log**.

tempcomp

Esta opción registra las mediciones de temperatura y las compensaciones de velocidad del sistema en un archivo llamado **tempcomp.log**.
Los archivos de registro se escriben en el directorio especificado por el comando **logdir**.

Un ejemplo del comando es:

```
registro de mediciones seguimiento de estadísticas
```

logdir

Esta directiva permite especificar el directorio donde se escriben los archivos de registro.
Un ejemplo del uso de esta directiva es:

```
logdir /var/log/chrony
```

hace un paso

Normalmente, **chronyd** hará que el sistema corrija gradualmente cualquier desfase temporal, ralentizando o acelerando el reloj según sea necesario. En determinadas situaciones, el reloj del sistema puede estar tan desviado que este proceso de giro tardaría mucho tiempo en corregir el reloj del sistema. Esta directiva obliga a **chronyd** a acelerar el reloj del sistema si el ajuste es mayor que un valor umbral, pero sólo si no hubo más actualizaciones del reloj desde que se inició **chronyd** que un límite especificado (se puede utilizar un valor negativo para desactivar el límite). Esto es particularmente útil cuando se utiliza el reloj de referencia, porque la directiva **initstepslew** sólo funciona con fuentes **NTP**.
Un ejemplo del uso de esta directiva es:

```
makestep 1000 10
```

Esto haría que el reloj del sistema se adelantara si el ajuste es mayor de 1000 segundos, pero sólo en las primeras diez actualizaciones del reloj.

maxchange

Esta directiva establece el máximo desplazamiento permitido corregido en una actualización del reloj. La comprobación se realiza sólo después del número especificado de actualizaciones para permitir un gran ajuste inicial del reloj del sistema. Cuando se produce un desfase mayor que el máximo especificado, se ignorará durante el número de veces especificado y luego **chronyd** se dará por vencido y saldrá (se puede utilizar un valor negativo para no salir nunca). En ambos casos se envía un mensaje a syslog.
Un ejemplo del uso de esta directiva es:

```
maxchange 1000 1 2
```

Después de la primera actualización del reloj, **chronyd** comprobará el desplazamiento en cada actualización del reloj, ignorará dos ajustes mayores de 1000 segundos y saldrá en otro.

maxupdateskew

Una de las tareas de **chronyd** es calcular lo rápido o lento que funciona el reloj del ordenador en relación con sus fuentes de referencia. Además, calcula una estimación de los límites de error en torno al valor estimado.
Si el rango de error es demasiado grande, indica que las mediciones aún no se han asentado y que la tasa de ganancia o pérdida estimada no es muy fiable.

El parámetro **maxupdateskew** es el umbral para determinar si una estimación es demasiado poco fiable para ser utilizada. Por defecto, el umbral es de 1000 ppm.

El formato de la sintaxis es:

```
maxupdateskew skew-in-ppm
```

Los valores típicos de *skew-in-ppm* pueden ser 100 para una conexión telefónica con servidores a través de una línea telefónica, y 5 o 10 para un ordenador en una LAN.

Cabe señalar que éste no es el único medio de protección contra el uso de estimaciones poco fiables. En todo momento, **chronyd** mantiene un registro tanto de la tasa de ganancia o pérdida estimada, como del límite de error de la estimación. Cuando se genera una nueva estimación tras otra medición de una de las fuentes, se utiliza un algoritmo de combinación ponderada para actualizar la estimación maestra. Por lo tanto, si **chronyd** tiene una estimación maestra muy fiable y se genera una nueva estimación que tiene grandes límites de error, la estimación maestra existente dominará en la nueva estimación maestra.

minsources

La directiva **minsources** establece el número mínimo de fuentes que deben considerarse seleccionables en el algoritmo de selección de fuentes antes de que se actualice el reloj local.
El formato de la sintaxis es:

```
minsources number-of-sources
```

Por defecto, *number-of-sources* es 1. Establecer minsources a un número mayor puede servir para mejorar la fiabilidad, ya que varias fuentes tendrán que corresponder entre sí.

noclientlog

Esta directiva, que no toma argumentos, especifica que los accesos de los clientes no deben ser registrados. Normalmente se registran, lo que permite informar de las estadísticas mediante el comando clients en **chronyc** y permitir que los clientes utilicen el modo intercalado con la opción

xleave en la directiva **server**.

reselectdist

Cuando **chronyd** selecciona la fuente de sincronización entre las fuentes disponibles, preferirá la que tenga una distancia de sincronización mínima. Sin embargo, para evitar la reselección frecuente cuando hay fuentes con una distancia similar, se añade una distancia fija a la distancia de las fuentes que no están seleccionadas en ese momento. Esto se puede establecer con la opción **reselectdist**. Por defecto, la distancia es de 100 microsegundos.
El formato de la sintaxis es:

```
reselectdist dist-in-seconds
```

peso del estrato

La directiva **stratumweight** establece cuánta distancia debe añadirse por estrato a la distancia de sincronización cuando **chronyd** selecciona la fuente de sincronización entre las fuentes disponibles.
El formato de la sintaxis es:

```
peso del estrato dist-in-seconds
```

Por defecto, *dist-in-seconds* es de 1 milisegundo. Esto significa que las fuentes con un estrato más bajo suelen ser preferidas a las fuentes con un estrato más alto, incluso cuando su distancia es significativamente peor. Si se ajusta **stratumweight** a 0, **chronyd** ignora el estrato al seleccionar la fuente.

rtcfile

La directiva **rtcfile** define el nombre del archivo en el que **chronyd** puede guardar los parámetros asociados al seguimiento de la precisión del reloj en tiempo real (RTC) del sistema.
El formato de la sintaxis es:

```
rtcfile /var/lib/chrony/rtc
```

chronyd guarda la información en este archivo cuando sale y cuando se emite el comando **writertc** en **chronyc**. La información guardada es el error del RTC en alguna época, esa época (en segundos desde el 1 de enero de 1970), y la velocidad a la que el RTC gana o pierde tiempo. No todos los relojes de tiempo real están soportados ya que su código es específico del sistema. Tenga en cuenta que si se utiliza esta directiva, el reloj de tiempo real no debe ser ajustado manualmente, ya que esto interferiría con **chrony**para medir la velocidad a la que el reloj de tiempo real se desplaza si se ajusta a intervalos aleatorios.

rtcsync

La directiva **rtcsync** está presente en el archivo **/etc/chrony.conf** por defecto. Esto informará al kernel que el reloj del sistema se mantiene sincronizado y el kernel actualizará el reloj en tiempo real cada 11 minutos.

11.5.1. Configurar la seguridad de Chrony

chronyc puede acceder a **chronyd** de dos maneras:

- Protocolo de Internet, IPv4 o IPv6.
- Socket de dominio Unix, al que puede acceder localmente el usuario **root** o **chrony**.

Por defecto, **chronyc** se conecta al socket del dominio Unix. La ruta por defecto es **/var/run/chrony/chronyd.sock**. Si esta conexión falla, lo que puede ocurrir por ejemplo cuando **chronyc** se ejecuta bajo un usuario no root, **chronyc** intenta conectarse a 127.0.0.1 y luego a ::1.

Sólo los siguientes comandos de supervisión, que no afectan al comportamiento de **chronyd**, están permitidos desde la red:

- actividad
- lista de manuales
- rtcdata
- alisado
- fuentes
- sourcestats
- rastreando
- waitsync

El conjunto de hosts de los que **chronyd** acepta estos comandos puede configurarse con la directiva **cmdallow** en el archivo de configuración de **chronyd**, o el comando **cmdallow** en **chronyc**. Por defecto, los comandos se aceptan sólo desde localhost (127.0.0.1 o ::1).

Todos los demás comandos sólo se permiten a través del socket de dominio Unix. Cuando se envía a través de la red, **chronyd** responde con un error **Not authorised**, incluso si es desde localhost.

Acceder a chronyd de forma remota conchronyc

1. Permita el acceso desde direcciones IPv4 e IPv6 añadiendo lo siguiente al archivo **/etc/chrony.conf**:

   ```
   bindcmdaddress 0.0.0.0
   ```

   o

   ```
   bindcmdaddress ::
   ```

2. Permitir comandos desde la dirección IP remota, red o subred utilizando la directiva **cmdallow**. Añada el siguiente contenido al archivo **/etc/chrony.conf**:

   ```
   cmdallow 192.168.1.0/24
   ```

3. Abra el puerto 323 en el firewall para conectarse desde un sistema remoto.

   ```
   # firewall-cmd --zone=public --add-port=323/udp
   ```

   Si desea abrir el puerto 323 de forma permanente, utilice la dirección **--permanent**.

   ```
   # firewall-cmd --permanent --zone=public --add-port=323/udp
   ```

Tenga en cuenta que la directiva **allow** es para el acceso a **NTP** mientras que la directiva **cmdallow** es

para permitir la recepción de comandos remotos. Es posible hacer estos cambios temporalmente usando **chronyc** ejecutando localmente. Edite el archivo de configuración para hacer cambios permanentes.

11.6. USO DE CHRONY

11.6.1. Instalación de crono

La suite **chrony** está instalado por defecto en Red Hat Enterprise Linux. Para asegurarse de que lo está, ejecute el siguiente comando como **root**:

```
# yum install chrony
```

La ubicación por defecto del **chrony** daemon es **/usr/sbin/chronyd**. La utilidad de línea de comandos se instalará en **/usr/bin/chronyc**.

11.6.2. Comprobación del estado de chronyd

Para comprobar el estado de **chronyd**, emita el siguiente comando:

```
$ systemctl status chronyd
chronyd.service - NTP client/server
   Loaded: loaded (/usr/lib/systemd/system/chronyd.service; enabled)
   Active: active (running) since Wed 2013-06-12 22:23:16 CEST; 11h ago
```

11.6.3. Inicio de la crónica

Para iniciar **chronyd**, emita el siguiente comando como **root**:

```
# systemctl start chronyd
```

Para garantizar que **chronyd** se inicie automáticamente al arrancar el sistema, emita el siguiente comando como **root**:

```
# systemctl enable chronyd
```

11.6.4. Detener la cronicidad

Para detener **chronyd**, emita el siguiente comando como **root**:

```
# systemctl stop chronyd
```

Para evitar que **chronyd** se inicie automáticamente al arrancar el sistema, emita el siguiente comando como **root**:

```
# systemctl disable chronyd
```

11.6.5. Comprobación de la sincronización de la cronía

Para comprobar si **chrony** está sincronizado, utilice los comandos **tracking**, **sources**, y **sourcestats**.

11.6.5.1. Comprobación del seguimiento de las crónicas

Para comprobar el **chrony** el seguimiento, emita el siguiente comando:

```
$ chronyc tracking
Reference ID    : CB00710F (foo.example.net)
Stratum         : 3
Ref time (UTC)  : Fri Jan 27 09:49:17 2017
System time     :  0.000006523 seconds slow of NTP time
Last offset     : -0.000006747 seconds
RMS offset      : 0.000035822 seconds
Frequency       : 3.225 ppm slow
Residual freq   : 0.000 ppm
Skew            : 0.129 ppm
Root delay      : 0.013639022 seconds
Root dispersion : 0.001100737 seconds
Update interval : 64.2 seconds
Leap status     : Normal
```

Los campos son los siguientes:

ID de referencia

Es el ID de referencia y el nombre (o la dirección **IP**), si está disponible, del servidor con el que el ordenador está sincronizado actualmente. El ID de referencia es un número hexadecimal para evitar confusiones con las direcciones IPv4.

Estrato

El estrato indica a cuántos saltos estamos de un ordenador con un reloj de referencia conectado. Un ordenador de este tipo es un ordenador de estrato 1, por lo que el ordenador del ejemplo está a dos saltos (es decir, a.b.c es un estrato 2 y se sincroniza desde un estrato 1).

Tiempo de referencia

Es la hora (UTC) a la que se procesó la última medición de la fuente de referencia.

Tiempo del sistema

En el funcionamiento normal, **chronyd** nunca acelera el reloj del sistema, porque cualquier salto en la escala de tiempo puede tener consecuencias adversas para ciertos programas de aplicación. En su lugar, cualquier error en el reloj del sistema se corrige acelerando o ralentizando ligeramente el reloj del sistema hasta que el error se haya eliminado, y luego volviendo a la velocidad normal del reloj del sistema. Una consecuencia de esto es que habrá un período en el que el reloj del sistema (leído por otros programas que utilizan la llamada al sistema **gettimeofday()**, o por el comando date en el shell) será diferente de la estimación de **chronyd** de la hora real actual (que informa a los clientes de **NTP** cuando está operando en modo servidor). El valor informado en esta línea es la diferencia debida a este efecto.

Última compensación

Es el desplazamiento local estimado en la última actualización del reloj.

Desplazamiento RMS

Se trata de una media a largo plazo del valor de compensación.

Frecuencia

La "frecuencia" es la velocidad con la que el reloj del sistema se equivocaría si **chronyd** no lo corrigiera. Se expresa en ppm (partes por millón). Por ejemplo, un valor de 1 ppm significaría que cuando el reloj del sistema cree que ha avanzado 1 segundo, en realidad ha avanzado 1,000001 segundos respecto al tiempo real.

Frecuencia residual

Muestra la "frecuencia residual" de la fuente de referencia seleccionada actualmente. Refleja cualquier diferencia entre lo que las mediciones de la fuente de referencia indican que debería ser la frecuencia y la frecuencia que se está utilizando actualmente.

La razón por la que no siempre es cero es que se aplica un procedimiento de suavizado a la frecuencia. Cada vez que se obtiene una medición de la fuente de referencia y se calcula una nueva frecuencia residual, la precisión estimada de este residuo se compara con la precisión estimada (véase **skew**) del valor de la frecuencia existente. Se calcula una media ponderada para la nueva frecuencia, con pesos que dependen de estas precisiones. Si las mediciones de la fuente de referencia siguen una tendencia consistente, el residuo se llevará a cero con el tiempo.

Inclinación

Es el límite de error estimado de la frecuencia.

Retraso de la raíz

Es el total de los retrasos de la ruta de la red hacia el ordenador del estrato 1 desde el que se sincroniza finalmente el ordenador. Los valores de retardo de la raíz se imprimen en resolución de nanosegundos. En ciertas situaciones extremas, este valor puede ser negativo. (Esto puede surgir en una disposición de pares simétricos en la que las frecuencias de los ordenadores no se siguen entre sí y el retardo de la red es muy corto en relación con el tiempo de giro en cada ordenador)

Dispersión de las raíces

Se trata de la dispersión total acumulada a través de todos los ordenadores hasta el ordenador del estrato 1 desde el que se sincroniza finalmente el ordenador. La dispersión se debe a la resolución del reloj del sistema, a las variaciones estadísticas de las mediciones, etc. Los valores de dispersión de la raíz se imprimen en resolución de nanosegundos.

Estado del salto

Este es el estado del salto, que puede ser Normal, Insertar segundo, Borrar segundo o No sincronizado.

11.6.5.2. Comprobación de las fuentes de crono

El comando sources muestra información sobre las fuentes de tiempo actuales a las que **chronyd** está accediendo.

Se puede especificar el argumento opcional -v, que significa verboso. En este caso, se muestran líneas de subtítulos adicionales como recordatorio de los significados de las columnas.

```
$ chronyc sources
 210 Number of sources = 3
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================

#* GPS0                          0   4   377    11   -479ns[ -621ns] /-  134ns
^? a.b.c                        2   6   377    23   -923us[ -924us] +/-   43ms
^ d.e.f                       1   6   377    21  -2629us[-2619us] +/-   86ms
```

Las columnas son las siguientes:

M

Indica el modo de la fuente. **^** significa un servidor, **=** significa un peer y **#** indica un reloj de referencia conectado localmente.

S

Esta columna indica el estado de las fuentes. \ "*" indica la fuente con la que **chronyd** está sincronizada actualmente. " " indica las fuentes aceptables que se combinan con la fuente

seleccionada. "-" indica las fuentes aceptables que son excluidas por el algoritmo de combinación. "?" indica las fuentes con las que se ha perdido la conectividad o cuyos paquetes no superan todas las pruebas. \ "x" indica un reloj que **chronyd** piensa que es un *falseticker* (su tiempo es inconsistente con la mayoría de las otras fuentes). "~" indica una fuente cuya hora parece tener demasiada variabilidad. La condición "?" también se muestra al inicio, hasta que se hayan recogido al menos 3 muestras de ella.

Nombre/dirección IP

Muestra el nombre o la dirección **IP** de la fuente, o el ID de referencia para el reloj de referencia.

Estrato

Muestra el estrato de la fuente, tal y como se informa en su última muestra recibida. El estrato 1 indica un ordenador con un reloj de referencia conectado localmente. Un ordenador sincronizado con un ordenador de estrato 1 está en el estrato 2. Un ordenador sincronizado con un ordenador de estrato 2 está en el estrato 3, y así sucesivamente.

Encuesta

Indica la velocidad a la que se sondea la fuente, como logaritmo de base 2 del intervalo en segundos. Así, un valor de 6 indicaría que se está realizando una medición cada 64 segundos.
chronyd varía automáticamente la tasa de sondeo en función de las condiciones existentes.

Llegar a

Esto muestra el registro de alcance de la fuente impreso como un número octal. El registro tiene 8 bits y se actualiza en cada paquete recibido o perdido de la fuente. Un valor de 377 indica que se recibió una respuesta válida para todas las últimas ocho transmisiones.

LastRx

Esta columna muestra cuánto tiempo hace que se recibió la última muestra de la fuente. Normalmente se indica en segundos. Las letras **m**, **h**, **d** o **y** indican minutos, horas, días o años. Un valor de 10 años indica que aún no se han recibido muestras de esta fuente.

Última muestra

Esta columna muestra el desfase entre el reloj local y la fuente en la última medición. El número entre corchetes muestra el desfase real medido. Puede llevar el sufijo **ns** (que indica nanosegundos), **us** (que indica microsegundos), **ms** (que indica milisegundos) o **s** (que indica segundos). El número que aparece a la izquierda de los corchetes muestra la medición original, ajustada para tener en cuenta los giros aplicados al reloj local desde entonces. El número que sigue al indicador **/-** muestra el margen de error de la medición. Los desfases positivos indican que el reloj local está adelantado con respecto a la fuente.

11.6.5.3. Comprobación de las estadísticas de la fuente de cronos

El comando **sourcestats** muestra información sobre el proceso de estimación de la tasa de deriva y el desplazamiento para cada una de las fuentes que se están examinando actualmente en **chronyd**.

Se puede especificar el argumento opcional **-v**, que significa verboso. En este caso, se muestran líneas de subtítulos adicionales como recordatorio de los significados de las columnas.

```
$ chronyc sourcestats
210 Number of sources = 1
Name/IP Address            NP  NR  Span  Frequency  Freq Skew  Offset  Std Dev
==============================================================================

abc.def.ghi                11   5   46m     -0.001      0.045     1us    25us
```

Las columnas son las siguientes:

Nombre/dirección IP

Es el nombre o la dirección **IP** del servidor **NTP** (o peer) o el ID de referencia del reloj de referencia al que se refiere el resto de la línea.

NP

Es el número de puntos de muestreo que se conservan actualmente para el servidor. La tasa de deriva y el desplazamiento actual se estiman realizando una regresión lineal a través de estos puntos.

NR

Es el número de ejecuciones de residuos que tienen el mismo signo después de la última regresión. Si este número empieza a ser demasiado pequeño en relación con el número de muestras, indica que la línea recta ya no se ajusta bien a los datos. Si el número de ejecuciones es demasiado bajo, **chronyd** descarta las muestras más antiguas y vuelve a ejecutar la regresión hasta que el número de ejecuciones sea aceptable.

Span

Es el intervalo entre las muestras más antiguas y las más recientes. Si no se muestra ninguna unidad, el valor está en segundos. En el ejemplo, el intervalo es de 46 minutos.

Frecuencia

Es la frecuencia residual estimada para el servidor, en partes por millón. En este caso, se estima que el reloj del ordenador funciona 1 parte en 10^9 lento en relación con el servidor.

Freq Skew

Se trata de los límites de error estimados en Freq (de nuevo en partes por millón).

Desplazamiento

Es el desplazamiento estimado de la fuente.

Desviación estándar

Se trata de la desviación estándar estimada de la muestra.

11.6.6. Ajuste manual del reloj del sistema

Para ajustar el reloj del sistema inmediatamente, omitiendo cualquier ajuste en curso por giro, emita el siguiente comando como **root**:

```
# chronyc makestep
```

Si se utiliza la directiva **rtcfile**, el reloj en tiempo real no debe ajustarse manualmente. Los ajustes aleatorios interferirían con **chrony**para medir la velocidad a la que se desplaza el reloj en tiempo real.

11.7. CONFIGURACIÓN DEL CRONO PARA DIFERENTES ENTORNOS

11.7.1. Configuración de la crónica para un sistema en una red aislada

En una red que nunca está conectada a Internet, se selecciona un ordenador para que sea el servidor de tiempo maestro. Los otros ordenadores son clientes directos del maestro, o clientes de clientes. En el maestro, el archivo de deriva debe configurarse manualmente con la tasa media de deriva del reloj del sistema. Si el maestro se reinicia, obtendrá la hora de los sistemas circundantes y calculará una media para ajustar su reloj de sistema. A partir de entonces, reanudará la aplicación de los ajustes basándose en el archivo de desviación. El archivo de desviación se actualizará automáticamente cuando se utilice el comando **settime**.

En el sistema seleccionado como maestro, utilizando un editor de texto que se ejecute como **root**, edite **/etc/chrony.conf** como sigue:

```
driftfile /var/lib/chrony/drift
commandkey 1
keyfile /etc/chrony.keys
initstepslew 10 client1 client3 client6
local stratum 8
manual
allow 192.0.2.0
```

Donde **192.0.2.0** es la dirección de red o subred desde la que los clientes pueden conectarse.

En los sistemas seleccionados para ser clientes directos del maestro, utilizando un editor de texto que se ejecute como **root**, edite el **/etc/chrony.conf** como sigue:

```
server master
driftfile /var/lib/chrony/drift
logdir /var/log/chrony
log measurements statistics tracking
keyfile /etc/chrony.keys
commandkey 24
local stratum 10
initstepslew 20 master
allow 192.0.2.123
```

Donde **192.0.2.123** es la dirección del maestro, y **master** es el nombre de host del maestro. Los clientes con esta configuración resincronizarán el maestro si se reinicia.

En los sistemas cliente que no van a ser clientes directos del maestro, el archivo **/etc/chrony.conf** debe ser el mismo, salvo que deben omitirse las directivas **local** y **allow**.

En una red aislada, también se puede utilizar la directiva **local** que habilita un modo de referencia local, que permite que **chronyd** que funciona como un servidor **NTP** aparezca sincronizado con el tiempo real, incluso cuando nunca fue sincronizado o la última actualización del reloj ocurrió hace mucho tiempo.

Para permitir que varios servidores de la red utilicen la misma configuración local y se sincronicen entre sí, sin confundir a los clientes que sondean más de un servidor, utilice la opción **orphan** de la directiva **local**, que activa el modo huérfano. Cada servidor debe estar configurado para sondear todos los demás servidores con **local**. Esto asegura que sólo el servidor con el ID de referencia más pequeño tiene la referencia local activa y los demás servidores se sincronizan con él. Cuando el servidor falle, otro tomará el relevo.

11.8. CRONÍA CON MARCA DE TIEMPO HW

11.8.1. Comprender la marca de tiempo del hardware

El sellado de tiempo por hardware es una característica soportada en algunos Controladores de Interfaz de Red (NIC) que proporciona un sellado de tiempo preciso de los paquetes entrantes y salientes. **NTP** los sellos de tiempo son creados generalmente por el kernel y **chronyd** con el uso del reloj del sistema. Sin embargo, cuando el timestamping HW está habilitado, el NIC utiliza su propio reloj para generar las marcas de tiempo cuando los paquetes entran o salen de la capa de enlace o de la capa física. Cuando se utiliza con **NTP**, el timestamping por hardware puede mejorar significativamente la precisión de la sincronización. Para obtener la máxima precisión, tanto los servidores de **NTP** como los clientes de **NTP** deben utilizar marcas de tiempo por hardware. En condiciones ideales, puede ser posible una precisión inferior al microsegundo.

Otro protocolo de sincronización horaria que utiliza la marca de tiempo por hardware es **PTP**.

A diferencia de **NTP**, **PTP** depende de la asistencia de los conmutadores y enrutadores de la red. Si quiere alcanzar la mejor precisión de sincronización, utilice **PTP** en redes que tengan conmutadores y enrutadores con soporte de **PTP**, y prefiera **NTP** en redes que no tengan tales conmutadores y enrutadores.

11.8.2. Verificación de la compatibilidad con la marca de tiempo del hardware

Para verificar que una interfaz admite el sellado de tiempo por hardware con **NTP**, utilice el comando **ethtool -T**. Se puede utilizar una interfaz para el timestamping por hardware con **NTP** si **ethtool** enumera las capacidades de **SOF_TIMESTAMPING_TX_HARDWARE** y **SOF_TIMESTAMPING_TX_SOFTWARE** y también el modo de filtro **HWTSTAMP_FILTER_ALL**.

Ejemplo 11.1. Verificación de la compatibilidad con la marca de tiempo por hardware en una interfaz específica

```
# ethtool -T eth0
```

La salida:

```
Timestamping parameters for eth0:
Capabilities:
        hardware-transmit     (SOF_TIMESTAMPING_TX_HARDWARE)
        software-transmit     (SOF_TIMESTAMPING_TX_SOFTWARE)
        hardware-receive      (SOF_TIMESTAMPING_RX_HARDWARE)
        software-receive      (SOF_TIMESTAMPING_RX_SOFTWARE)
        software-system-clock (SOF_TIMESTAMPING_SOFTWARE)
        hardware-raw-clock    (SOF_TIMESTAMPING_RAW_HARDWARE)
PTP Hardware Clock: 0
Hardware Transmit Timestamp Modes:
        off                   (HWTSTAMP_TX_OFF)
        on                    (HWTSTAMP_TX_ON)
Hardware Receive Filter Modes:
        none                  (HWTSTAMP_FILTER_NONE)
        all                   (HWTSTAMP_FILTER_ALL)
        ptpv1-l4-sync         (HWTSTAMP_FILTER_PTP_V1_L4_SYNC)
        ptpv1-l4-delay-req    (HWTSTAMP_FILTER_PTP_V1_L4_DELAY_REQ)
        ptpv2-l4-sync         (HWTSTAMP_FILTER_PTP_V2_L4_SYNC)
        ptpv2-l4-delay-req    (HWTSTAMP_FILTER_PTP_V2_L4_DELAY_REQ)
        ptpv2-l2-sync         (HWTSTAMP_FILTER_PTP_V2_L2_SYNC)
        ptpv2-l2-delay-req    (HWTSTAMP_FILTER_PTP_V2_L2_DELAY_REQ)
        ptpv2-event           (HWTSTAMP_FILTER_PTP_V2_EVENT)
        ptpv2-sync            (HWTSTAMP_FILTER_PTP_V2_SYNC)
        ptpv2-delay-req       (HWTSTAMP_FILTER_PTP_V2_DELAY_REQ)
```

11.8.3. Activación de la marca de tiempo por hardware

Para activar la marca de tiempo por hardware, utilice la directiva **hwtimestamp** en el archivo **/etc/chrony.conf**. La directiva puede especificar una sola interfaz, o se puede utilizar un carácter comodín para habilitar el timestamping por hardware en todas las interfaces que lo soporten. Utilice la

especificación de comodín en caso de que ninguna otra aplicación, como **ptp4l** del paquete **linuxptp**, utilice el timestamping por hardware en una interfaz. Se permiten múltiples directivas **hwtimestamp** en el archivo de configuración de chrony.

Ejemplo 11.2. Activación de la marca de tiempo por hardware mediante la directiva hwtimestamp

```
hwtimestamp eth0
hwtimestamp eth1
hwtimestamp *
```

11.8.4. Configuración del intervalo de sondeo del cliente

El intervalo de sondeo por defecto (64-1024 segundos) se recomienda para servidores en Internet. En el caso de los servidores locales y de las marcas de tiempo por hardware, es necesario configurar un intervalo de sondeo más corto para minimizar el desfase del reloj del sistema.

La siguiente directiva en **/etc/chrony.conf** especifica un servidor local **NTP** utilizando un intervalo de sondeo de un segundo:

```
servidor ntp.local minpoll 0 maxpoll 0
```

11.8.5. Activación del modo intercalado

NTP que no son dispositivos de hardware **NTP**, sino ordenadores de propósito general que ejecutan una implementación de software **NTP**, como **chrony**obtendrán una marca de tiempo de transmisión por hardware sólo después de enviar un paquete. Este comportamiento impide que el servidor guarde la marca de tiempo en el paquete al que corresponde. Para permitir que los clientes de **NTP** reciban marcas de tiempo de transmisión generadas después de la transmisión, configure los clientes para que utilicen el modo intercalado de **NTP** añadiendo la opción **xleave** a la directiva del servidor en **/etc/chrony.conf**:

```
servidor ntp.local minpoll 0 maxpoll 0 xleave
```

11.8.6. Configuración del servidor para un gran número de clientes

La configuración por defecto del servidor permite que unos pocos miles de clientes, como máximo, utilicen el modo intercalado simultáneamente. Para configurar el servidor para un mayor número de clientes, aumente la directiva **clientloglimit** en **/etc/chrony.conf**. Esta directiva especifica el tamaño máximo de la memoria asignada para el registro de los accesos de los clientes en el servidor:

```
clientloglimit 100000000
```

11.8.7. Verificación de la marca de tiempo del hardware

Para verificar que la interfaz ha habilitado con éxito el timestamping por hardware, compruebe el registro del sistema. El registro debería contener un mensaje de **chronyd** para cada interfaz con el timestamping de hardware activado correctamente.

Ejemplo 11.3. Mensajes de registro para las interfaces con la marca de tiempo de hardware activada

```
```

```
chronyd[4081]: Enabled HW timestamping on eth0
chronyd[4081]: Enabled HW timestamping on eth1
```

Cuando **chronyd** está configurado como un cliente o peer de **NTP**, puede hacer que se informen los modos de timestamping de transmisión y recepción y el modo intercalado para cada fuente de **NTP** mediante el comando **chronyc ntpdata**:

Ejemplo 11.4. Informar sobre la transmisión, la recepción y el modo intercalado de cada fuente NTP

```
# chronyc ntpdata
```

La salida:

```
Remote address  : 203.0.113.15 (CB00710F)
Remote port     : 123
Local address   : 203.0.113.74 (CB00714A)
Leap status     : Normal
Version         : 4
Mode            : Server
Stratum         : 1
Poll interval   : 0 (1 seconds)
Precision       : -24 (0.000000060 seconds)
Root delay      : 0.000015 seconds
Root dispersion : 0.000015 seconds
Reference ID    : 47505300 (GPS)
Reference time  : Wed May 03 13:47:45 2017
Offset          : -0.000000134 seconds
Peer delay      : 0.000005396 seconds
Peer dispersion : 0.000002329 seconds
Response time   : 0.000152073 seconds
Jitter asymmetry: +0.00
NTP tests       : 111 111 1111
Interleaved     : Yes
Authenticated   : No
TX timestamping : Hardware
RX timestamping : Hardware
Total TX        : 27
Total RX        : 27
Total valid RX  : 27
```

Ejemplo 11.5. Informar sobre la estabilidad de las mediciones NTP

```
# chronyc sourcestats
```

Con la marca de tiempo del hardware activada, la estabilidad de las mediciones de **NTP** debería estar en decenas o cientos de nanosegundos, bajo carga normal. Esta estabilidad se indica en la columna **Std Dev** de la salida del comando **chronyc sourcestats**:

La salida:

```
210 Number of sources = 1
Name/IP Address            NP  NR  Span  Frequency  Freq Skew  Offset  Std Dev
ntp.local                  12   7    11     +0.000      0.019     +0ns    49ns
```

11.8.8. Configuración del puente PTP-NTP

Si se dispone de un gran maestro del Protocolo de Tiempo de Precisión (**PTP**) de alta precisión en una red que no tiene conmutadores o enrutadores con soporte de **PTP**, se puede dedicar un ordenador para que funcione como esclavo de **PTP** y como servidor de estrato-1 **NTP**. Este ordenador debe tener dos o más interfaces de red y estar cerca del gran maestro o tener una conexión directa con él. Esto garantizará una sincronización muy precisa en la red.

Configurar el **ptp4l** y **phc2sys** de los paquetes **linuxptp** para que utilicen una interfaz para sincronizar el reloj del sistema mediante **PTP**.

Configure **chronyd** para proporcionar la hora del sistema utilizando la otra interfaz:

Ejemplo 11.6. Configuración de chronyd para proporcionar la hora del sistema utilizando la otra interfaz

```
bindaddress 203.0.113.74
hwtimestamp eth1
local stratum 1
```

11.9. CONSEGUIR ALGUNOS AJUSTES QUE ANTES SOPORTABA NTP EN CHRONY

Algunas configuraciones que estaban en la versión principal anterior de Red Hat Enterprise Linux soportadas por **ntp**no son compatibles con **chrony**. Esta sección enumera tales configuraciones y describe las formas de lograrlas en un sistema con **chrony**.

11.9.1. Monitorización mediante ntpq y ntpdc

chronyd no puede ser controlado por el **ntpq** y **ntpdc** de la distribución **ntp** porque **chrony** no soporta los modos 6 y 7 de **NTP**. Soporta un protocolo diferente y **chronyc** es la implementación del cliente. Para más información, consulte la página man de **chronyc(1)**.

Para controlar el estado del reloj del sistema sincronizado por **chronyd**, puede:

- Utilice el comando de seguimiento
- Utilice la **ntpstat** que es compatible con **chrony** y proporciona una salida similar a la que se obtenía con **ntpd**

Ejemplo 11.7. Utilizar el comando de seguimiento

```
$ chronyc -n tracking
Reference ID    : 0A051B0A (10.5.27.10)
Stratum         : 2
Ref time (UTC)  : Thu Mar 08 15:46:20 2018
```

```
System time     : 0.000000338 seconds slow of NTP time
Last offset     : +0.000339408 seconds
RMS offset      : 0.000339408 seconds
Frequency       : 2.968 ppm slow
Residual freq   : +0.001 ppm
Skew            : 3.336 ppm
Root delay      : 0.157559142 seconds
Root dispersion : 0.001339232 seconds
Update interval : 64.5 seconds
Leap status     : Normal
```

Ejemplo 11.8. Uso de la utilidad ntpstat

```
$ ntpstat
synchronised to NTP server (10.5.27.10) at stratum 2
   time correct to within 80 ms
   polling server every 64 s
```

11.9.2. Utilización de un mecanismo de autenticación basado en la criptografía de clave pública

En Red Hat Enterprise Linux 7, **ntp** soporta **Autokey**que es un mecanismo de autenticación basado en criptografía de clave pública **Autokey** no está soportado en **chronyd**.

En un sistema Red Hat Enterprise Linux 8, se recomienda utilizar claves simétricas. Genere las claves con el comando **chronyc keygen**. Un cliente y un servidor necesitan compartir una clave especificada en **/etc/chrony.keys**. El cliente puede habilitar la autenticación utilizando la opción **key** en la directiva **server**, **pool**, o **peer**.

11.9.3. Uso de asociaciones simétricas efímeras

En Red Hat Enterprise Linux 7, **ntpd** soportaba asociaciones simétricas efímeras, que pueden ser movilizadas por paquetes de pares que no están especificados en el archivo de configuración **ntp.conf**. En Red Hat Enterprise Linux 8, **chronyd** necesita que todos los pares sean especificados en **chrony.conf**. Las asociaciones simétricas efímeras no son soportadas.

Tenga en cuenta que el uso del modo cliente/servidor activado por la directiva **server** o **pool** es más seguro en comparación con el modo simétrico activado por la directiva **peer**.

11.9.4. cliente de multidifusión/transmisión

Red Hat Enterprise Linux 7 soporta el modo broadcast/multicast **NTP**, que simplifica la configuración de los clientes. Con este modo, los clientes pueden ser configurados para que sólo escuchen los paquetes enviados a una dirección de multidifusión/difusión en lugar de escuchar nombres o direcciones específicas de servidores individuales, que pueden cambiar con el tiempo.

En Red Hat Enterprise Linux 8, **chronyd** no soporta el modo de difusión/multidifusión. La razón principal es que es menos preciso y menos seguro que los modos ordinarios cliente/servidor y simétrico.

Hay varias opciones de migración desde una configuración de emisión/multidifusión de **NTP**:

- Configurar el DNS para traducir un solo nombre, como ntp.ejemplo.com, a varias direcciones de diferentes servidores
  Los clientes pueden tener una configuración estática utilizando sólo una directiva de pool para sincronizar con varios servidores. Si un servidor del pool se vuelve irrecuperable, o no es apto para la sincronización, los clientes lo sustituyen automáticamente por otro servidor del pool.

- Distribuir la lista de servidores **NTP** a través de DHCP
  Cuando NetworkManager obtiene una lista de servidores **NTP** del servidor DHCP, **chronyd** se configura automáticamente para utilizarlos. Esta función puede desactivarse añadiendo **PEERNTP=no** al archivo **/etc/sysconfig/network**.

- Utilice el **Precision Time Protocol (PTP)**
  Esta opción es adecuada principalmente para entornos en los que los servidores cambian con frecuencia, o si un grupo más grande de clientes necesita poder sincronizarse entre sí sin tener un servidor designado.

  PTP fue diseñado para la mensajería multidifusión y funciona de forma similar al modo de difusión **NTP**. Una implementación de **PTP** está disponible en el paquete **linuxptp**.

  para que**PTP** funcione bien, es necesario contar con marcas de tiempo por hardware y soporte en los conmutadores de red. Sin embargo, se espera que **PTP** funcione mejor que **NTP** en el modo de difusión, incluso con marca de tiempo por software y sin soporte en los conmutadores de red.

  En redes con un gran número de esclavos **PTP** en una ruta de comunicación, se recomienda configurar los esclavos **PTP** con la opción **hybrid_e2e** para reducir la cantidad de tráfico de red generado por los esclavos. Se puede configurar un ordenador que ejecute **chronyd** como cliente de **NTP**, y posiblemente como servidor de **NTP**, para que funcione también como gran maestro de **PTP** y distribuya la hora sincronizada a un gran número de ordenadores utilizando la mensajería multicast.

11.10. RECURSOS ADICIONALES

Las siguientes fuentes de información ofrecen recursos adicionales sobre **chrony**.

11.10.1. Documentación instalada

- **chronyc(1)** página de manual - Describe la **chronyc** herramienta de interfaz de línea de comandos, incluyendo los comandos y las opciones de comando.

- **chronyd(8)** página de manual - Describe el demonio **chronyd** incluyendo comandos y opciones de comando.

- **chrony.conf(5)** página de manual - Describe el **chrony** archivo de configuración.

11.10.2. Documentación en línea

- https://chrony.tuxfamily.org/doc/3.3/chronyc.html

- https://chrony.tuxfamily.org/doc/3.3/chronyd.html

- https://chrony.tuxfamily.org/doc/3.3/chrony.conf.html

Las respuestas a las preguntas más frecuentes se encuentran en https://chrony.tuxfamily.org/faq.html

11.11. GESTIÓN DE LA SINCRONIZACIÓN HORARIA MEDIANTE LOS ROLES DE SISTEMA DE RHEL

Puede gestionar la sincronización horaria en varios equipos de destino utilizando el rol **timesync**.

El rol **timesync** instala y configura una implementación NTP o PTP para operar como cliente NTP o esclavo PTP para sincronizar el reloj del sistema con servidores NTP o grandes maestros en dominios PTP.

Tenga en cuenta que el uso del rol **timesync** también facilita la migración a chrony, porque puede utilizar el mismo playbook en todas las versiones de Red Hat Enterprise Linux a partir de RHEL 6, independientemente de si el sistema utiliza **ntp** o **chrony** para implementar el protocolo NTP.

AVISO

El rol **timesync** reemplaza la configuración del servicio del proveedor dado o detectado en el host gestionado. Las configuraciones anteriores se pierden, incluso si no están especificadas en las variables del rol. La única configuración conservada es la elección del proveedor si la variable **timesync_ntp_provider** no está definida.

El siguiente ejemplo muestra cómo aplicar la función **timesync** en una situación con un solo grupo de servidores.

Ejemplo 11.9. Un ejemplo de libro de jugadas aplicando la función timesync para un único grupo de servidores

```
---
- hosts: timesync-test
  vars:
    timesync_ntp_servers:
      - hostname: 2.rhel.pool.ntp.org
        pool: yes
        iburst: yes
  roles:
    - rhel-system-roles.timesync
```

Recursos adicionales

- Para una referencia detallada sobre las variables de rol de **timesync**, instale el paquete **rhel-system-roles**, y vea los archivos **README.md** o **README.html** en el directorio **/usr/share/doc/rhel-system-roles/timesync**.
- Para más información sobre los roles de sistema de RHEL, consulte Introducción a los roles de sistema de RHEL.

CAPÍTULO 12. USO DE COMUNICACIONES SEGURAS ENTRE DOS SISTEMAS CON OPENSSH

SSH (Secure Shell) es un protocolo que proporciona comunicaciones seguras entre dos sistemas utilizando una arquitectura cliente-servidor y permite a los usuarios iniciar la sesión en los sistemas anfitriones del servidor de forma remota. A diferencia de otros protocolos de comunicación remota, como FTP o Telnet, SSH cifra la sesión de inicio de sesión, lo que impide que los intrusos recojan las contraseñas no cifradas de la conexión.

Red Hat Enterprise Linux incluye los paquetes básicos **OpenSSH**: el paquete general **openssh**, el paquete **openssh-server** y el paquete **openssh-clients**. Tenga en cuenta que los paquetes **OpenSSH** requieren el paquete **OpenSSL openssl-libs** , que instala varias bibliotecas criptográficas importantes que permiten a **OpenSSH** proporcionar comunicaciones cifradas.

12.1. SSH Y OPENSSH

SSH (Secure Shell) es un programa para entrar en una máquina remota y ejecutar comandos en esa máquina. El protocolo SSH proporciona comunicaciones seguras y encriptadas entre dos hosts no confiables a través de una red insegura. También puede reenviar conexiones X11 y puertos TCP/IP arbitrarios a través del canal seguro.

El protocolo SSH mitiga las amenazas de seguridad, como la interceptación de la comunicación entre dos sistemas y la suplantación de un determinado host, cuando se utiliza para el inicio de sesión de shell remoto o la copia de archivos. Esto se debe a que el cliente y el servidor SSH utilizan firmas digitales para verificar sus identidades. Además, toda la comunicación entre los sistemas cliente y servidor está cifrada.

OpenSSH es una implementación del protocolo SSH soportada por varios sistemas operativos Linux, UNIX y similares. Incluye los archivos centrales necesarios para el cliente y el servidor de OpenSSH. La suite OpenSSH consiste en las siguientes herramientas de espacio de usuario:

- **ssh** es un programa de acceso remoto (cliente SSH)
- **sshd** es un demonio SSH **OpenSSH**
- **scp** es un programa de copia remota segura de archivos
- **sftp** es un programa de transferencia segura de archivos
- **ssh-agent** es un agente de autenticación para el almacenamiento de claves privadas
- **ssh-add** añade identidades de clave privada a **ssh-agent**
- **ssh-keygen** genera, gestiona y convierte las claves de autenticación para **ssh**
- **ssh-copy-id** es un script que añade claves públicas locales al archivo **authorized_keys** en un servidor SSH remoto
- **ssh-keyscan** - recoge las claves públicas de host SSH

Actualmente existen dos versiones de SSH: la versión 1 y la versión 2, más reciente. La suite **OpenSSH** en Red Hat Enterprise Linux 8 sólo soporta la versión 2 de SSH, que tiene un algoritmo de intercambio de claves mejorado que no es vulnerable a los exploits conocidos de la versión 1.

OpenSSH, como uno de los subsistemas criptográficos centrales de RHEL, utiliza políticas criptográficas para todo el sistema. Esto asegura que los conjuntos de cifrado y los algoritmos

criptográficos débiles están desactivados en la configuración por defecto. Para ajustar la política, el administrador debe utilizar el comando **update-crypto-policies** para hacer la configuración más estricta o más floja o excluir manualmente las políticas criptográficas de todo el sistema.

El conjunto **OpenSSH** utiliza dos conjuntos diferentes de archivos de configuración: los de los programas cliente (es decir, **ssh**, **scp**, y **sftp**), y los del servidor (el demonio **sshd**). La información de configuración de SSH para todo el sistema se almacena en el directorio **/etc/ssh/**. La información de configuración SSH específica del usuario se almacena en **~/.ssh/** en el directorio de inicio del usuario. Para una lista detallada de los archivos de configuración de OpenSSH, vea la sección **FILES** en la página man **sshd(8)**.

Recursos adicionales

- Páginas de manual para el tema **ssh** listadas por el comando **man -k ssh**.
- Uso de políticas criptográficas en todo el sistema .

12.2. CONFIGURAR E INICIAR UN SERVIDOR OPENSSH

Utilice el siguiente procedimiento para una configuración básica que puede ser necesaria para su entorno y para iniciar un servidor **OpenSSH**. Tenga en cuenta que después de la instalación por defecto de RHEL, el demonio **sshd** ya está iniciado y las claves del servidor se crean automáticamente.

Requisitos previos

- El paquete **openssh-server** está instalado.

Procedimiento

1. Inicie el demonio **sshd** en la sesión actual y configúrelo para que se inicie automáticamente al arrancar:

```
# systemctl start sshd
# systemctl enable sshd
```

2. Para especificar direcciones diferentes a las predeterminadas **0.0.0.0** (IPv4) o **::** (IPv6) para la directiva **ListenAddress** en el archivo de configuración **/etc/ssh/sshd_config** y utilizar una configuración de red dinámica más lenta, añada la dependencia de la unidad de destino **network-online.target** al archivo de unidad **sshd.service**. Para ello, cree el archivo **/etc/systemd/system/sshd.service.d/local.conf** con el siguiente contenido:

```
[Unit]
Wants=network-online.target
After=network-online.target
```

3. Revise si la configuración del servidor **OpenSSH** en el archivo de configuración **/etc/ssh/sshd_config** cumple con los requisitos de su escenario.

4. Opcionalmente, cambie el mensaje de bienvenida que su servidor **OpenSSH** muestra antes de que un cliente se autentique editando el archivo **/etc/issue**, por ejemplo:

```
Welcome to ssh-server.example.com
Warning: By accessing this server, you agree to the referenced terms and conditions.
```

Asegúrese de que la opción **Banner** no está comentada en **/etc/ssh/sshd_config** y su valor contiene **/etc/issue**:

```
# less /etc/ssh/sshd_config | grep Banner
Banner /etc/issue
```

Tenga en cuenta que para cambiar el mensaje que se muestra después de un inicio de sesión exitoso tiene que editar el archivo **/etc/motd** en el servidor. Consulte la página man **pam_motd** para obtener más información.

5. Vuelva a cargar la configuración de **systemd** y reinicie **sshd** para aplicar los cambios:

```
# systemctl daemon-reload
# systemctl restart sshd
```

Pasos de verificación

1. Compruebe que el demonio **sshd** se está ejecutando:

```
# 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 2019-11-18 14:59:58 CET; 6min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 1149 (sshd)
    Tasks: 1 (limit: 11491)
   Memory: 1.9M
   CGroup: /system.slice/sshd.service
           └─1149 /usr/sbin/sshd -D -oCiphers=aes128-ctr,aes256-ctr,aes128-cbc,aes256-cbc -
oMACs=hmac-sha2-256,>

Nov 18 14:59:58 ssh-server-example.com systemd[1]: Starting OpenSSH server daemon...
Nov 18 14:59:58 ssh-server-example.com sshd[1149]: Server listening on 0.0.0.0 port 22.
Nov 18 14:59:58 ssh-server-example.com sshd[1149]: Server listening on :: port 22.
Nov 18 14:59:58 ssh-server-example.com systemd[1]: Started OpenSSH server daemon.
```

2. Conéctese al servidor SSH con un cliente SSH.

```
# ssh user@ssh-server-example.com
ECDSA key fingerprint is SHA256:dXbaS0RG/UzlTTku8GtXSz0S1++lPegSy31v3L/FAEc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ssh-server-example.com' (ECDSA) to the list of known hosts.

user@ssh-server-example.com's password:
```

Recursos adicionales

- **sshd(8)** y **sshd_config(5)** páginas man

12.3. USO DE PARES DE CLAVES EN LUGAR DE CONTRASEÑAS PARA LA AUTENTICACIÓN SSH

Para mejorar aún más la seguridad del sistema, genere pares de claves SSH y luego aplique la autenticación basada en claves deshabilitando la autenticación por contraseña.

12.3.1. Configuración de un servidor OpenSSH para la autenticación basada en claves

Siga estos pasos para configurar su servidor OpenSSH para aplicar la autenticación basada en claves.

Requisitos previos

- El paquete **openssh-server** está instalado.
- El demonio **sshd** se está ejecutando en el servidor.

Procedimiento

1. Abra la configuración de **/etc/ssh/sshd_config** en un editor de texto, por ejemplo:

```
# vi /etc/ssh/sshd_config
```

2. Cambie la opción **PasswordAuthentication** por **no**:

```
PasswordAuthentication no
```

   En un sistema que no sea una instalación nueva por defecto, compruebe que no se ha configurado **PubkeyAuthentication no** y que la directiva **ChallengeResponseAuthentication** está establecida en **no**. Si está conectado de forma remota, sin utilizar la consola o el acceso fuera de banda, pruebe el proceso de inicio de sesión basado en la clave antes de desactivar la autenticación por contraseña.

3. Para utilizar la autenticación basada en claves con los directorios personales montados en NFS, active el booleano **use_nfs_home_dirs** SELinux:

```
# setsebool -P use_nfs_home_dirs 1
```

4. Vuelva a cargar el demonio **sshd** para aplicar los cambios:

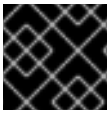
```
# systemctl reload sshd
```

Recursos adicionales

- **sshd(8)**, **sshd_config(5)**, y **setsebool(8)** páginas de manual

12.3.2. Generación de pares de claves SSH

Utilice este procedimiento para generar un par de claves SSH en un sistema local y para copiar la clave pública generada en un servidor **OpenSSH**. Si el servidor está configurado como corresponde, podrá iniciar sesión en el servidor **OpenSSH** sin necesidad de proporcionar ninguna contraseña.



IMPORTANTE

Si completa los siguientes pasos como **root**, sólo **root** podrá utilizar las llaves.

Procedimiento

1. Para generar un par de claves ECDSA para la versión 2 del protocolo SSH:

```
$ ssh-keygen -t ecdsa
Generating public/private ecdsa key pair.
Enter file in which to save the key (/home/joesec/.ssh/id_ecdsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/joesec/.ssh/id_ecdsa.
Your public key has been saved in /home/joesec/.ssh/id_ecdsa.pub.
The key fingerprint is:
SHA256:Q/x+qms4j7PCQ0qFd09iZEFHA+SqwBKRNaU72oZfaCI
joesec@localhost.example.com
The key's randomart image is:
+---[ECDSA 256]---+
|.oo..o=++        |
|.. o .oo .       |
|. .. o. o        |
|....o.+...       |
|o.oo.o +S .      |
|.=.+.   .o       |
|E.*+.  .  . .    |
|.=..+ +..  o     |
|  .  oo*+o.      |
+----[SHA256]-----+
```

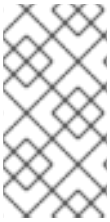
También puede generar un par de claves RSA utilizando la opción **-t rsa** con el comando **ssh-keygen** o un par de claves Ed25519 introduciendo el comando **ssh-keygen -t ed25519**.

2. Para copiar la clave pública en una máquina remota:

```
$ ssh-copy-id joesec@ssh-server-example.com
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are
already installed
joesec@ssh-server-example.com's password:
...
Number of key(s) added: 1

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

Si no utiliza el programa **ssh-agent** en su sesión, el comando anterior copia la clave pública más recientemente modificada **~/.ssh/id*.pub** si aún no está instalada. Para especificar otro archivo de clave pública o para dar prioridad a las claves en archivos sobre las claves almacenadas en la memoria por **ssh-agent**, utilice el comando **ssh-copy-id** con la opción **-i**.



NOTA

Si reinstalas tu sistema y quieres conservar los pares de claves generados anteriormente, haz una copia de seguridad del directorio **~/.ssh/**. Después de reinstalar, cópialo de nuevo en tu directorio principal. Puedes hacer esto para todos los usuarios de tu sistema, incluyendo **root**.

Pasos de verificación

1. Inicie sesión en el servidor OpenSSH sin proporcionar ninguna contraseña:

```
$ ssh joesec@ssh-server-example.com
Welcome message.
...
Last login: Mon Nov 18 18:28:42 2019 from ::1
```

Recursos adicionales

- **ssh-keygen(1)** y **ssh-copy-id(1)** páginas man

12.4. USO DE CLAVES SSH ALMACENADAS EN UNA TARJETA INTELIGENTE

Red Hat Enterprise Linux 8 le permite utilizar claves RSA y ECDSA almacenadas en una tarjeta inteligente en clientes OpenSSH. Utilice este procedimiento para habilitar la autenticación utilizando una tarjeta inteligente en lugar de utilizar una contraseña.

Requisitos previos

- En el lado del cliente, el paquete **opensc** está instalado y el servicio **pcscd** está funcionando.

Procedimiento

1. Enumerar todas las claves proporcionadas por el módulo PKCS #11 de OpenSC incluyendo sus URIs PKCS #11 y guardar el resultado en el archivo *keys.pub*:

```
$ ssh-keygen -D pkcs11: > keys.pub
$ ssh-keygen -D pkcs11:
ssh-rsa AAAAB3NzaC1yc2E...KKZMzcQZzx
pkcs11:id=%02;object=SIGN%20pubkey;token=SSH%20key;manufacturer=piv_II?module-
path=/usr/lib64/pkcs11/opensc-pkcs11.so
ecdsa-sha2-nistp256 AAA...J0hkYnnsM=
pkcs11:id=%01;object=PIV%20AUTH%20pubkey;token=SSH%20key;manufacturer=piv_II?
module-path=/usr/lib64/pkcs11/opensc-pkcs11.so
```

2. Para habilitar la autenticación mediante una tarjeta inteligente en un servidor remoto (*example.com*), transfiera la clave pública al servidor remoto. Utilice el comando **ssh-copy-id** con *keys.pub* creado en el paso anterior:

```
$ ssh-copy-id -f -i keys.pub username@example.com
```

3. Para conectarse a *example.com* utilizando la clave ECDSA de la salida del comando **ssh-keygen -D** en el paso 1, puede utilizar sólo un subconjunto de la URI, que hace referencia a su clave de forma exclusiva, por ejemplo:

```
$ ssh -i "pkcs11:id=%01?module-path=/usr/lib64/pkcs11/opensc-pkcs11.so" example.com
Enter PIN for 'SSH key':
[example.com] $
```

4. Puede utilizar la misma cadena URI en el archivo **~/.ssh/config** para que la configuración sea permanente:

```
$ cat ~/.ssh/config
```

```
IdentityFile "pkcs11:id=%01?module-path=/usr/lib64/pkcs11/opensc-pkcs11.so"
$ ssh example.com
Enter PIN for 'SSH key':
[example.com] $
```

Dado que OpenSSH utiliza el wrapper **p11-kit-proxy** y el módulo PKCS #11 de OpenSC está registrado en PKCS#11 Kit, puede simplificar los comandos anteriores:

```
$ ssh -i "pkcs11:id=%01" example.com
Enter PIN for 'SSH key':
[example.com] $
```

Si se omite la parte **id=** de un URI PKCS #11, OpenSSH carga todas las claves que están disponibles en el módulo proxy. Esto puede reducir la cantidad de escritura requerida:

```
$ ssh -i pkcs11: example.com
Enter PIN for 'SSH key':
[example.com] $
```

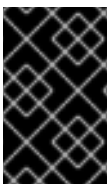
Recursos adicionales

- Fedora 28: Mejor soporte para tarjetas inteligentes en OpenSSH
- **p11-kit(8)** página de manual
- **ssh(1)** página de manual
- **ssh-keygen(1)** página de manual
- **opensc.conf(5)** página de manual
- **pcscd(8)** página de manual

12.5. CÓMO HACER QUE OPENSSH SEA MÁS SEGURO

Los siguientes consejos le ayudarán a aumentar la seguridad cuando utilice OpenSSH. Tenga en cuenta que los cambios en el archivo de configuración de **/etc/ssh/sshd_config** OpenSSH requieren la recarga del demonio **sshd** para que surtan efecto:

```
# systemctl reload sshd
```



IMPORTANTE

La mayoría de los cambios en la configuración del refuerzo de la seguridad reducen la compatibilidad con los clientes que no admiten algoritmos o conjuntos de cifrado actualizados.

Desactivación de los protocolos de conexión inseguros

- Para que SSH sea realmente eficaz, hay que evitar el uso de protocolos de conexión inseguros que sean sustituidos por el conjunto **OpenSSH**. De lo contrario, la contraseña de un usuario podría estar protegida usando SSH para una sesión sólo para ser capturada más tarde cuando

se conecte usando Telnet. Por esta razón, considere deshabilitar los protocolos inseguros, como telnet, rsh, rlogin y ftp.

Activación de la autenticación basada en clave y desactivación de la autenticación basada en contraseña

- Desactivar las contraseñas para la autenticación y permitir sólo los pares de claves reduce la superficie de ataque y también podría ahorrar tiempo a los usuarios. En los clientes, genere pares de claves utilizando la herramienta **ssh-keygen** y utilice la utilidad **ssh-copy-id** para copiar las claves públicas de los clientes en el servidor **OpenSSH**. Para desactivar la autenticación basada en contraseña en su servidor OpenSSH, edite **/etc/ssh/sshd_config** y cambie la opción **PasswordAuthentication** por **no**:

```
PasswordAuthentication no
```

Tipos de claves

- Aunque el comando **ssh-keygen** genera un par de claves RSA por defecto, puedes indicarle que genere claves ECDSA o Ed25519 utilizando la opción **-t**. El ECDSA (Algoritmo de Firma Digital de Curva Elíptica) ofrece un mejor rendimiento que el RSA con una fuerza de clave simétrica equivalente. También genera claves más cortas. El algoritmo de clave pública Ed25519 es una implementación de curvas de Edwards retorcidas que es más segura y también más rápida que RSA, DSA y ECDSA.
  OpenSSH crea automáticamente las claves de host del servidor RSA, ECDSA y Ed25519 si no las tiene. Para configurar la creación de claves de host en RHEL 8, utilice el servicio instanciado **sshd-keygen@.service**. Por ejemplo, para desactivar la creación automática del tipo de clave RSA:

```
# systemctl mask sshd-keygen@rsa.service
```

- Para excluir determinados tipos de claves para las conexiones SSH, comente las líneas correspondientes en **/etc/ssh/sshd_config** y vuelva a cargar el servicio **sshd**. Por ejemplo, para permitir sólo las claves de host Ed25519:

```
# HostKey /etc/ssh/ssh_host_rsa_key
# HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
```

Puerto no predeterminado

- Por defecto, el demonio **sshd** escucha en el puerto TCP 22. Cambiar el puerto reduce la exposición del sistema a ataques basados en el escaneo automático de la red y, por tanto, aumenta la seguridad a través de la oscuridad. Puede especificar el puerto utilizando la directiva **Port** en el archivo de configuración **/etc/ssh/sshd_config**.
  También tienes que actualizar la política por defecto de SELinux para permitir el uso de un puerto no predeterminado. Para ello, utilice la herramienta **semanage** del paquete **policycoreutils-python-utils**:

```
# semanage port -a -t ssh_port_t -p tcp port_number
```

  Además, actualice la configuración de **firewalld**:

```
# firewall-cmd --add-port port_number/tcp
# firewall-cmd --runtime-to-permanent
```

En los comandos anteriores, sustituya *port_number* por el nuevo número de puerto especificado mediante la directiva **Port**.

No hay acceso a la raíz

- Si su caso de uso particular no requiere la posibilidad de iniciar sesión como usuario root, debería considerar establecer la directiva de configuración **PermitRootLogin** a **no** en el archivo **/etc/ssh/sshd_config**. Al deshabilitar la posibilidad de iniciar sesión como usuario root, el administrador puede auditar qué usuarios ejecutan qué comandos privilegiados después de iniciar sesión como usuarios normales y luego obtener derechos de root.
  Como alternativa, configure **PermitRootLogin** en **prohibit-password**:

  ```
  PermitRootLogin prohibir-contraseña
  ```

  Esto refuerza el uso de la autenticación basada en claves en lugar del uso de contraseñas para iniciar la sesión como root y reduce los riesgos al evitar los ataques de fuerza bruta.

Uso de la extensión X Security

- El servidor X en los clientes de Red Hat Enterprise Linux no proporciona la extensión X Security. Por lo tanto, los clientes no pueden solicitar otra capa de seguridad cuando se conectan a servidores SSH no confiables con el reenvío X11. La mayoría de las aplicaciones no pueden ejecutarse con esta extensión habilitada de todos modos.
  Por defecto, la opción **ForwardX11Trusted** en el archivo **/etc/ssh/ssh_config.d/05-redhat.conf** se establece en **yes**, y no hay diferencia entre el comando **ssh -X remote_machine** (host no confiable) y **ssh -Y remote_machine** (host confiable).

  Si su escenario no requiere la función de reenvío de X11 en absoluto, establezca la directiva **X11Forwarding** en el archivo de configuración **/etc/ssh/sshd_config** a **no**.

Restringir el acceso a usuarios, grupos o dominios específicos

- Las directivas **AllowUsers** y **AllowGroups** en el archivo de configuración del servidor **/etc/ssh/sshd_config** le permiten permitir sólo a ciertos usuarios, dominios o grupos conectarse a su servidor OpenSSH. Puede combinar **AllowUsers** y **AllowGroups** para restringir el acceso con mayor precisión, por ejemplo:

  ```
  AllowUsers *@192.168.1.*,*@10.0.0.*,!*@192.168.1.2
  AllowGroups example-group
  ```

  Las líneas de configuración anteriores aceptan conexiones de todos los usuarios de los sistemas de las subredes 192.168.1.* y 10.0.0.*, excepto del sistema con la dirección 192.168.1.2. Todos los usuarios deben estar en el grupo **example-group**. El servidor OpenSSH rechaza todas las demás conexiones.

  Tenga en cuenta que el uso de listas de permitidos (directivas que empiezan por Allow) es más seguro que el uso de listas de bloqueados (opciones que empiezan por Deny) porque las listas de permitidos bloquean también a nuevos usuarios o grupos no autorizados.

Cambiar las políticas criptográficas de todo el sistema

- **OpenSSH** utiliza las políticas criptográficas de todo el sistema RHEL, y el nivel de política criptográfica por defecto de todo el sistema ofrece una configuración segura para los modelos de amenazas actuales. Para que la configuración criptográfica sea más estricta, cambie el nivel de política actual:

```
# update-crypto-policies --set FUTURE
Setting system policy to FUTURE
```

- Para optar por las políticas de criptografía de todo el sistema para su servidor **OpenSSH**, descomente la línea con la variable **CRYPTO_POLICY=** en el archivo **/etc/sysconfig/sshd**. Después de este cambio, los valores que especifique en las secciones **Ciphers**, **MACs**, **KexAlgoritms**, y **GSSAPIKexAlgorithms** en el archivo **/etc/ssh/sshd_config** no serán anulados. Tenga en cuenta que esta tarea requiere una gran experiencia en la configuración de opciones criptográficas.

- Consulte Uso de políticas criptográficas en todo el sistema en el título de endurecimiento de la seguridad de RHEL 8 para obtener más información.

Recursos adicionales

- **sshd_config(5)**, **ssh-keygen(1)**, **crypto-policies(7)**, y **update-crypto-policies(8)** páginas de manual

12.6. CONECTARSE A UN SERVIDOR REMOTO UTILIZANDO UN HOST DE SALTO SSH

Utilice este procedimiento para conectarse a un servidor remoto a través de un servidor intermediario, también llamado host de salto.

Requisitos previos

- Un host de salto acepta conexiones SSH desde su sistema.
- Un servidor remoto acepta conexiones SSH sólo desde el host de salto.

Procedimiento

1. Defina el host de salto editando el archivo **~/.ssh/config**, por ejemplo:

```
Host jump-server1
  HostName jump1.example.com
```

2. Añada la configuración de salto del servidor remoto con la directiva **ProxyJump** a **~/.ssh/config**, por ejemplo:

```
Host remote-server
  HostName remote1.example.com
  ProxyJump jump-server1
```

3. Conectar con el servidor remoto a través del servidor de salto:

```
$ ssh remote-server
```

El comando anterior es equivalente al comando **ssh -J jump-server1 remote-server** si se omiten los pasos de configuración 1 y 2.

NOTA

Puede especificar más servidores de salto y también puede omitir la adición de definiciones de host al archivo de configuraciones cuando proporciona sus nombres de host completos, por ejemplo:

```
$ ssh -J jump1.example.com,jump2.example.com,jump3.example.com
remote1.example.com
```

Cambie la notación de sólo nombre de host en el comando anterior si los nombres de usuario o los puertos SSH en los servidores de salto difieren de los nombres y puertos en el servidor remoto, por ejemplo:

```
$ ssh -J
johndoe@jump1.example.com:75,johndoe@jump2.example.com:75,johndoe@jump3.e
xample.com:75 joesec@remote1.example.com:220
```

Recursos adicionales

- **ssh_config(5)** y **ssh(1)** páginas man

12.7. CONEXIÓN A MÁQUINAS REMOTAS CON CLAVES SSH USANDO SSH-AGENT

Para evitar la introducción de una frase de contraseña cada vez que inicie una conexión SSH, puede utilizar la utilidad **ssh-agent** para almacenar en caché la clave privada SSH. La clave privada y la frase de contraseña permanecen seguras.

Requisitos previos

- Tienes un host remoto con el demonio SSH en ejecución y accesible a través de la red.
- Conoce la dirección IP o el nombre de host y las credenciales para iniciar sesión en el host remoto.
- Ha generado un par de claves SSH con una frase de paso y ha transferido la clave pública a la máquina remota. Para más información, consulte Generación de pares de claves SSH.

Procedimiento

1. Opcional: Compruebe que puede utilizar la clave para autenticarse en el host remoto:
   a. Conéctese al host remoto mediante SSH:

      ```
      $ ssh example.user1@198.51.100.1 hostname
      ```

   b. Introduzca la frase de contraseña que estableció al crear la clave para dar acceso a la clave privada.

```
$ ssh example.user1@198.51.100.1 hostname
 host.example.com
```

2. Inicie el **ssh-agent**.

```
$ eval $(ssh-agent)
Agent pid 20062
```

3. Añade la clave a **ssh-agent**.

```
$ ssh-add ~/.ssh/id_rsa
Enter passphrase for ~/.ssh/id_rsa:
Identity added: ~/.ssh/id_rsa (example.user0@198.51.100.12)
```

Pasos de verificación

- Opcional: Inicie sesión en el equipo anfitrión mediante SSH.

```
$ ssh example.user1@198.51.100.1

Last login: Mon Sep 14 12:56:37 2020
```

Tenga en cuenta que no ha tenido que introducir la frase de contraseña.

12.8. RECURSOS ADICIONALES

Para obtener más información sobre la configuración y la conexión a los servidores y clientes de **OpenSSH** en Red Hat Enterprise Linux, consulte los recursos enumerados a continuación.

Documentación instalada

- **sshd(8)** La página de manual documenta las opciones disponibles en la línea de comandos y proporciona una lista completa de los archivos y directorios de configuración compatibles.
- la página de manual**ssh(1)** proporciona una lista completa de las opciones disponibles en la línea de comandos y de los archivos y directorios de configuración admitidos.
- la página de manual**scp(1)** proporciona una descripción más detallada de la utilidad **scp** y su uso.
- la página de manual**sftp(1)** proporciona una descripción más detallada de la utilidad **sftp** y su uso.
- la página man**ssh-keygen(1)** documenta en detalle el uso de la utilidad **ssh-keygen** para generar, gestionar y convertir las claves de autenticación utilizadas por ssh.
- la página de manual**ssh-copy-id(1)** describe el uso del script **ssh-copy-id**.
- **ssh_config(5)** La página de manual documenta las opciones de configuración del cliente SSH disponibles.
- la página de manual**sshd_config(5)** proporciona una descripción completa de las opciones de configuración disponibles del demonio SSH.

- la página de manual**update-crypto-policies(8)** proporciona orientación sobre la gestión de políticas criptográficas en todo el sistema
- la página de manual**crypto-policies(7)** proporciona una visión general de los niveles de política criptográfica de todo el sistema

Documentación en línea

- Página principal de OpenSSH: contiene más documentación, preguntas frecuentes, enlaces a las listas de correo, informes de errores y otros recursos útiles.
- Configuración de SELinux para aplicaciones y servicios con configuraciones no estándar: puede aplicar procedimientos análogos para OpenSSH en una configuración no estándar con SELinux en modo de refuerzo.
- Controlar el tráfico de la red utilizando firewalld - proporciona orientación sobre la actualización de la configuración de **firewalld** después de cambiar un puerto SSH

CAPÍTULO 13. CONFIGURACIÓN DE UNA SOLUCIÓN DE REGISTRO REMOTO

Para garantizar que los registros de varias máquinas de su entorno se registren de forma centralizada en un servidor de registro, puede configurar la aplicación **Rsyslog** para que registre los registros que se ajusten a criterios específicos desde el sistema cliente al servidor.

13.1. EL SERVICIO DE REGISTRO RSYSLOG

La aplicación Rsyslog, en combinación con el servicio **systemd-journald**, proporciona soporte de registro local y remoto en Red Hat Enterprise Linux. El demonio **rsyslogd** lee continuamente los mensajes **syslog** recibidos por el servicio **systemd-journald** desde el diario. **rsyslogd** luego filtra y procesa estos eventos **syslog** y los registra en archivos de registro **rsyslog** o los reenvía a otros servicios según su configuración.

El demonio **rsyslogd** también proporciona filtrado ampliado, retransmisión de mensajes protegida por encriptación, módulos de entrada y salida, y soporte para el transporte mediante los protocolos TCP y UDP.

En **/etc/rsyslog.conf**, que es el archivo de configuración principal para **rsyslog**, puede especificar las reglas según las cuales **rsyslogd** maneja los mensajes. En general, puede clasificar los mensajes por su origen y tema (facilidad) y urgencia (prioridad), y luego asignar una acción que debe realizarse cuando un mensaje se ajusta a estos criterios.

En **/etc/rsyslog.conf**, también puede ver una lista de archivos de registro mantenidos por **rsyslogd**. La mayoría de los archivos de registro se encuentran en el directorio **/var/log/**. Algunas aplicaciones, como **httpd** y **samba**, almacenan sus archivos de registro en un subdirectorio dentro de **/var/log/**.

Recursos adicionales

- Las páginas de manual **rsyslogd(8)** y **rsyslog.conf(5)**
- Documentación instalada con el paquete **rsyslog-doc** en file:///usr/share/doc/rsyslog/html/index.html

13.2. INSTALACIÓN DE LA DOCUMENTACIÓN DE RSYSLOG

La aplicación Rsyslog tiene una amplia documentación que está disponible en https://www.rsyslog.com/doc/, pero también puede instalar el paquete de documentación **rsyslog-doc** localmente siguiendo este procedimiento.

Requisitos previos

- Ha activado el repositorio **AppStream** en su sistema
- Está autorizado a instalar nuevos paquetes mediante **sudo**

Procedimiento

- Instale el paquete **rsyslog-doc**:

```
$ sudo yum install rsyslog-doc
```

Verificación

Verificación

- Abra el archivo file:///usr/share/doc/rsyslog/html/index. html en un navegador de su elección, por ejemplo:

```
$ firefox file:///usr/share/doc/rsyslog/html/index.html
```

13.3. CONFIGURAR EL REGISTRO REMOTO A TRAVÉS DE TCP

La aplicación Rsyslog le permite tanto ejecutar un servidor de registro como configurar sistemas individuales para que envíen sus archivos de registro al servidor de registro. Para utilizar el registro remoto a través de TCP, configure tanto el servidor como el cliente. El servidor recoge y analiza los registros enviados por uno o varios sistemas cliente.

Con la aplicación Rsyslog, puede mantener un sistema de registro centralizado en el que los mensajes de registro se reenvían a un servidor a través de la red. Para evitar la pérdida de mensajes cuando el servidor no está disponible, puede configurar una cola de acción para la acción de reenvío. De este modo, los mensajes que no se han podido enviar se almacenan localmente hasta que el servidor vuelva a estar accesible. Tenga en cuenta que estas colas no pueden configurarse para las conexiones que utilizan el protocolo UDP.

El plug-in **omfwd** permite el reenvío a través de UDP o TCP. El protocolo por defecto es UDP. Como el complemento está incorporado, no es necesario cargarlo.

13.3.1. Configuración de un servidor para el registro remoto a través de TCP

Siga este procedimiento para configurar un servidor para recoger y analizar los registros enviados por uno o más sistemas cliente.

Por defecto, **rsyslog** utiliza TCP en el puerto **514**.

Requisitos previos

- **rsyslog** está instalado en el sistema del servidor
- Estás conectado como root en el servidor

Procedimiento

1. Opcional: Para utilizar un puerto diferente para el tráfico de **rsyslog**, añada el tipo de SELinux **syslogd_port_t** al puerto. Por ejemplo, habilite el puerto **30514**:

```
# semanage port -a -t syslogd_port_t -p tcp 30514
```

2. Opcional: Para utilizar un puerto diferente para el tráfico de **rsyslog**, configure **firewalld** para permitir el tráfico entrante de **rsyslog** en ese puerto. Por ejemplo, permita el tráfico TCP en el puerto **30514** en la zona **zone**:

```
# firewall-cmd --zone=zone --permanent --add-port=30514/tcp
success
```

3. Cree un nuevo archivo en el directorio **/etc/rsyslog.d/** llamado, por ejemplo, **remotelog.conf**, e inserte el siguiente contenido:

```
# Define templates before the rules that use them
### Per-Host Templates for Remote Systems ###
template(name="TmplAuthpriv" type="list") {
    constant(value="/var/log/remote/auth/")
    property(name="hostname")
    constant(value="/")
    property(name="programname" SecurePath="replace")
    constant(value=".log")
    }

template(name="TmplMsg" type="list") {
    constant(value="/var/log/remote/msg/")
    property(name="hostname")
    constant(value="/")
    property(name="programname" SecurePath="replace")
    constant(value=".log")
    }

# Provides TCP syslog reception
module(load="imtcp")
# Adding this ruleset to process remote messages
ruleset(name="remote1"){
     authpriv.*   action(type="omfile" DynaFile="TmplAuthpriv")
      *.info;mail.none;authpriv.none;cron.none
action(type="omfile" DynaFile="TmplMsg")
}

input(type="imtcp" port="30514" ruleset="remote1")
```

4. Guarde los cambios en el archivo **/etc/rsyslog.d/remotelog.conf**.

5. Asegúrese de que el servicio **rsyslog** se está ejecutando y está habilitado en el servidor de registro:

```
# systemctl status rsyslog
```

6. Reinicie el servicio **rsyslog**.

```
# systemctl restart rsyslog
```

7. Opcional: Si **rsyslog** no está habilitado, asegúrese de que el servicio **rsyslog** se inicie automáticamente tras el reinicio:

```
# systemctl enable rsyslog
```

Su servidor de registro está ahora configurado para recibir y almacenar archivos de registro de los otros sistemas de su entorno.

Verificación

- Pruebe la sintaxis del archivo **/etc/rsyslog.conf**:

```
# rsyslogd -N 1
rsyslogd: version 8.1911.0-2.el8, config validation run (level 1), master config
```

```
/etc/rsyslog.conf
rsyslogd: End of config validation run. Bye.
```

Recursos adicionales

- Las páginas de manual **rsyslogd(8)**, **rsyslog.conf(5)**, **semanage(8)**, y **firewall-cmd(1)**
- Documentación instalada con el paquete **rsyslog-doc** en file:///usr/share/doc/rsyslog/html/index.html

13.3.2. Configuración del registro remoto en un servidor a través de TCP

Siga este procedimiento para configurar un sistema de reenvío de mensajes de registro a un servidor a través del protocolo TCP. El complemento **omfwd** permite el reenvío a través de UDP o TCP. El protocolo por defecto es UDP. Como el complemento está incorporado, no es necesario cargarlo.

Requisitos previos

- El paquete **rsyslog** se instala en los sistemas cliente que deben informar al servidor.
- Ha configurado el servidor para el registro remoto.
- El puerto especificado está permitido en SELinux y abierto en el firewall.

Procedimiento

1. Cree un nuevo archivo en el directorio **/etc/rsyslog.d/** llamado, por ejemplo, **remotelog.conf**, e inserte el siguiente contenido:

```
*.* action(type="omfwd"
     queue.type="linkedlist"
     queue.filename="example_fwd"
     action.resumeRetryCount="-1"
     queue.saveOnShutdown="on"
     target="example.com" port="30514" protocol="tcp"
    )
```

Dónde:

- **queue.type="linkedlist"** habilita una cola LinkedList en memoria,
- **queue.filename** define un almacenamiento en disco. Los archivos de copia de seguridad se crean con el prefijo **example_fwd** en el directorio de trabajo especificado por la directiva global precedente **workDirectory**,
- la configuración de **action.resumeRetryCount -1** evita que **rsyslog** deje de enviar mensajes al reintentar conectarse si el servidor no responde,
- habilitado **queue.saveOnShutdown="on"** guarda los datos en memoria si **rsyslog** se apaga,
- la última línea reenvía todos los mensajes recibidos al servidor de registro, la especificación del puerto es opcional.

Con esta configuración, **rsyslog** envía mensajes al servidor pero mantiene los mensajes en la

memoria si el servidor remoto no está localizable. Sólo se crea un archivo en el disco si **rsyslog** se queda sin el espacio de cola de memoria configurado o necesita cerrarse, lo que beneficia el rendimiento del sistema.

2. Reinicie el servicio **rsyslog**.

```
# systemctl restart rsyslog
```

Verificación

Para verificar que el sistema cliente envía mensajes al servidor, siga estos pasos:

1. En el sistema cliente, envíe un mensaje de prueba:

```
# logger test
```

2. En el sistema del servidor, vea el registro **/var/log/messages**, por ejemplo:

```
# cat /var/log/remote/msg/hostname/root.log
Feb 25 03:53:17 hostname root[6064]: test
```

Donde *hostname* es el nombre del host del sistema cliente. Tenga en cuenta que el registro contiene el nombre del usuario que introdujo el comando **logger**, en este caso **root**.

Recursos adicionales

- Las páginas de manual **rsyslogd(8)** y **rsyslog.conf(5)**
- Documentación instalada con el paquete **rsyslog-doc** en file:///usr/share/doc/rsyslog/html/index.html

13.4. CONFIGURACIÓN DEL REGISTRO REMOTO A TRAVÉS DE UDP

La aplicación **Rsyslog** permite configurar un sistema para recibir información de registro de sistemas remotos. Para utilizar el registro remoto a través de UDP, configure tanto el servidor como el cliente. El servidor receptor recoge y analiza los registros enviados por uno o varios sistemas cliente. Por defecto, **rsyslog** utiliza UDP en el puerto **514** para recibir información de registro de sistemas remotos.

13.4.1. Configuración de un servidor para recibir información de registro remoto a través de UDP

Siga este procedimiento para configurar un servidor para recoger y analizar los registros enviados por uno o más sistemas cliente a través del protocolo UDP.

Requisitos previos

- La utilidad **rsyslog** está instalada.

Procedimiento

1. Opcional: Para utilizar un puerto diferente al predeterminado para el tráfico de **rsyslog 514** :
   a. Añade el tipo de SELinux **syslogd_port_t** a la configuración de la política de SELinux, sustituyendo ***portno*** por el número de puerto que quieres que use **rsyslog**:

```
# semanage port -a -t syslogd_port_t -p udp portno
```

b. Configure **firewalld** para permitir el tráfico entrante de **rsyslog**, sustituyendo ***portno*** por el número de puerto y **zone** por la zona que desea que utilice **rsyslog**:

```
# firewall-cmd --zone=zone --permanent --add-port=portno/udp
success
```

c. Recarga las reglas del firewall:

```
# firewall-cmd --reload
```

2. Cree un nuevo archivo **.conf** en el directorio **/etc/rsyslog.d/**, por ejemplo, **remotelogserv.conf**, e inserte el siguiente contenido:

```
# Define templates before the rules that use them
### Per-Host Templates for Remote Systems ###
template(name="TmplAuthpriv" type="list") {
    constant(value="/var/log/remote/auth/")
    property(name="hostname")
    constant(value="/")
    property(name="programname" SecurePath="replace")
    constant(value=".log")
    }

template(name="TmplMsg" type="list") {
    constant(value="/var/log/remote/msg/")
    property(name="hostname")
    constant(value="/")
    property(name="programname" SecurePath="replace")
    constant(value=".log")
    }

# Provides UDP syslog reception
module(load="imudp")

# This ruleset processes remote messages
ruleset(name="remote1"){
     authpriv.*   action(type="omfile" DynaFile="TmplAuthpriv")
      *.info;mail.none;authpriv.none;cron.none
action(type="omfile" DynaFile="TmplMsg")
}

input(type="imudp" port="514" ruleset="remote1")
```

Donde **514** es el número de puerto que **rsyslog** utiliza por defecto. Puede especificar un puerto diferente en su lugar.

3. Reinicie el servicio **rsyslog**.

```
# systemctl restart rsyslog
```

4. Opcional: Si **rsyslog** no está habilitado, asegúrese de que el servicio **rsyslog** se inicie automáticamente tras el reinicio:

```
# systemctl enable rsyslog
```

Verificación

1. Verifique la sintaxis del archivo **/etc/rsyslog.conf** y de todos los archivos **.conf** en el directorio **/etc/rsyslog.d/**:

```
# rsyslogd -N 1
rsyslogd: version 8.1911.0-2.el8, config validation run (level 1), master config
/etc/rsyslog.conf
rsyslogd: End of config validation run. Bye.
```

Recursos adicionales

- Las páginas de manual **rsyslogd(8)**, **rsyslog.conf(5)**, **semanage(8)**, y **firewall-cmd(1)**
- La documentación basada en el navegador, que puede instalar desde el paquete **rsyslog-doc**, en **file:///usr/share/doc/rsyslog/html/index.html**

13.4.2. Configurar el registro remoto en un servidor a través de UDP

Siga este procedimiento para configurar un sistema de reenvío de mensajes de registro a un servidor a través del protocolo UDP. El complemento **omfwd** permite el reenvío a través de UDP o TCP. El protocolo por defecto es UDP. Como el complemento está incorporado, no es necesario cargarlo.

Requisitos previos

- El paquete **rsyslog** se instala en los sistemas cliente que deben informar al servidor.
- Ha configurado el servidor para el registro remoto como se describe en Configuración de un servidor para recibir información de registro remoto a través de UDP.

Procedimiento

1. Cree un nuevo archivo **.conf** en el directorio **/etc/rsyslog.d/**, por ejemplo, **remotelogcli.conf**, e inserte el siguiente contenido:

```
*.* action(type="omfwd"
     queue.type="linkedlist"
     queue.filename="example_fwd"
     action.resumeRetryCount="-1"
     queue.saveOnShutdown="on"
     target="example.com" port="portno" protocol="udp"
    )
```

Dónde:

- **queue.type="linkedlist"** habilita una cola LinkedList en memoria.
- **queue.filename** define un almacenamiento en disco. Los archivos de copia de seguridad se crean con el ***example_fwd*** en el directorio de trabajo especificado por la directiva global anterior **workDirectory**.

- El ajuste **action.resumeRetryCount -1** evita que **rsyslog** deje de enviar mensajes al reintentar conectarse si el servidor no responde.
- **enabled queue.saveOnShutdown="on"** guarda los datos en memoria si **rsyslog** se apaga.
- ***portno*** es el número de puerto que quiere que utilice **rsyslog**. El valor por defecto es **514**.
- La última línea reenvía todos los mensajes recibidos al servidor de registro, la especificación del puerto es opcional.
  Con esta configuración, **rsyslog** envía mensajes al servidor pero mantiene los mensajes en la memoria si el servidor remoto no está localizable. Sólo se crea un archivo en el disco si **rsyslog** se queda sin el espacio de cola de memoria configurado o necesita cerrarse, lo que beneficia el rendimiento del sistema.

2. Reinicie el servicio **rsyslog**.

```
# systemctl restart rsyslog
```

3. Opcional: Si **rsyslog** no está habilitado, asegúrese de que el servicio **rsyslog** se inicie automáticamente tras el reinicio:

```
# systemctl enable rsyslog
```

Verificación

Para verificar que el sistema cliente envía mensajes al servidor, siga estos pasos:

1. En el sistema cliente, envíe un mensaje de prueba:

```
# logger test
```

2. En el sistema del servidor, vea el **/var/log/remote/msg/*hostname*/root.log** registro, por ejemplo:

```
# cat /var/log/remote/msg/hostname/root.log
Feb 25 03:53:17 hostname root[6064]: test
```

Donde **hostname** es el nombre del host del sistema cliente. Tenga en cuenta que el registro contiene el nombre del usuario que introdujo el comando del registrador, en este caso **root**.

Recursos adicionales

- Las páginas de manual **rsyslogd(8)** y **rsyslog.conf(5)**
- La documentación basada en el navegador, que puede instalar desde el paquete **rsyslog-doc**, en **file:///usr/share/doc/rsyslog/html/index.html**

13.5. CONFIGURACIÓN DE UN REGISTRO REMOTO FIABLE

Con el protocolo de registro de eventos fiable (RELP), puede enviar y recibir mensajes **syslog** a través de TCP con un riesgo mucho menor de pérdida de mensajes. RELP proporciona una entrega fiable de los mensajes de eventos, lo que lo hace útil en entornos donde la pérdida de mensajes no es aceptable. Para utilizar RELP, configure el módulo de entrada **imrelp**, que se ejecuta en el servidor y recibe los registros, y el módulo de salida **omrelp**, que se ejecuta en el cliente y envía los registros al servidor de registro.

Requisitos previos

- Ha instalado los paquetes **rsyslog**, **librelp**, y **rsyslog-relp** en el servidor y en los sistemas cliente.
- El puerto especificado está permitido en SELinux y abierto en el firewall.

Procedimiento

1. Configurar el sistema cliente para un registro remoto fiable:
   a. En el sistema cliente, cree un nuevo archivo **.conf** en el directorio /**etc**/**rsyslog.d**/ llamado, por ejemplo, **relpcli.conf**, e inserte el siguiente contenido:

```
module(load="omrelp")
*.* action(type="omrelp" target="target_IP" port="target_port")
```

   Dónde:

   - ***target_IP*** es la dirección IP del servidor de registro.
   - ***target_port*** es el puerto del servidor de registro.

   b. Guarde los cambios en el archivo /**etc**/**rsyslog.d**/**relpserv.conf**.
   c. Reinicie el servicio **rsyslog**.

```
# systemctl restart rsyslog
```

   d. Opcional: Si **rsyslog** no está habilitado, asegúrese de que el servicio **rsyslog** se inicie automáticamente tras el reinicio:

```
# systemctl enable rsyslog
```

2. Configurar el sistema del servidor para un registro remoto fiable:
   a. En el sistema del servidor, cree un nuevo archivo **.conf** en el directorio /**etc**/**rsyslog.d**/ llamado, por ejemplo, **relpserv.conf**, e inserte el siguiente contenido:

```
ruleset(name="relp"){
*.* action(type="omfile" file="log_path")
}


module(load="imrelp")
input(type="imrelp" port="target_port" ruleset="relp")
```

   Dónde:

   - ***log_path*** especifica la ruta para almacenar los mensajes.
   - ***target_port*** es el puerto del servidor de registro. Utilice el mismo valor que en el archivo de configuración del cliente.

   b. Guarde los cambios en el archivo /**etc**/**rsyslog.d**/**relpserv.conf**.

c. Reinicie el servicio **rsyslog**.

```
# systemctl restart rsyslog
```

d. Opcional: Si **rsyslog** no está habilitado, asegúrese de que el servicio **rsyslog** se inicie automáticamente tras el reinicio:

```
# systemctl enable rsyslog
```

Verificación

Para verificar que el sistema cliente envía mensajes al servidor, siga estos pasos:

1. En el sistema cliente, envíe un mensaje de prueba:

```
# logger test
```

2. En el sistema del servidor, vea el registro en la dirección especificada ***log_path***por ejemplo:

```
# cat /var/log/remote/msg/hostname/root.log
Feb 25 03:53:17 hostname root[6064]: test
```

Donde **hostname** es el nombre del host del sistema cliente. Tenga en cuenta que el registro contiene el nombre del usuario que introdujo el comando del registrador, en este caso **root**.

Recursos adicionales

- Las páginas de manual **rsyslogd(8)** y **rsyslog.conf(5)**
- La documentación basada en el navegador, que puede instalar desde el paquete **rsyslog-doc**, en **file:///usr/share/doc/rsyslog/html/index.html**

13.6. MÓDULOS RSYSLOG SOPORTADOS

Para ampliar la funcionalidad de la utilidad **Rsyslog**, puede utilizar módulos adicionales específicos. Los módulos proporcionan entradas adicionales (módulos de entrada), salidas (módulos de salida) y otras funcionalidades específicas. Un módulo también puede proporcionar directivas de configuración adicionales que están disponibles después de cargar ese módulo.

Liste los módulos de entrada y salida instalados en su sistema con el siguiente comando:

```
# ls /usr/lib64/rsyslog/{i,o}m#
```

Para ver la lista de todos los módulos disponibles en **rsyslog**, abra la siguiente página de documentación instalada desde el paquete **rsyslog-doc**.

```
$ firefox file:///usr/share/doc/rsyslog/html/configuration/modules/idx_output.html
```

13.7. RECURSOS ADICIONALES

- Documentación instalada con el paquete **rsyslog-doc** en file:///usr/share/doc/rsyslog/html/index.html

- Las páginas de manual **rsyslog.conf(5)** y **rsyslogd(8)**
- El artículo de la base de conocimientos Configurar el registro del sistema sin journald o con el uso minimizado de journald
- Los efectos negativos de la configuración de registro por defecto de RHEL en el rendimiento y sus mitigaciones artículo

CAPÍTULO 14. USO DE LA FUNCIÓN DE SISTEMA DE REGISTRO

Como administrador del sistema, puede utilizar el rol de sistema de registro para configurar un host RHEL como servidor de registro para recoger los registros de muchos sistemas cliente.

14.1. LA FUNCIÓN DEL SISTEMA DE REGISTRO

Con el rol de sistema de registro, puede desplegar configuraciones de registro en hosts locales y remotos.

Para aplicar un rol de sistema de registro en uno o más sistemas, se define la configuración de registro en un *playbook*. Un libro de jugadas es una lista de una o más jugadas. Los playbooks son legibles por humanos y están escritos en formato YAML. Para obtener más información sobre los libros de jugadas, consulte Trabajar con libros de jugadas en la documentación de Ansible.

El conjunto de sistemas que quiere que Ansible configure según el libro de jugadas se define en un *inventory file*. Para obtener más información sobre la creación y el uso de inventarios, consulte Cómo construir su inventario en la documentación de Ansible.

Las soluciones de registro proporcionan múltiples formas de leer los registros y múltiples salidas de registro.

Por ejemplo, un sistema de registro puede recibir las siguientes entradas:

- archivos locales,
- **systemd/journal**,
- otro sistema de registro a través de la red.

Además, un sistema de registro puede tener las siguientes salidas:

- los registros se almacenan en los archivos locales del directorio **/var/log**,
- los registros se envían a Elasticsearch,
- los registros se envían a otro sistema de registro.

Con el rol de sistema de registro, puedes combinar las entradas y salidas para adaptarlas a tus necesidades. Por ejemplo, puede configurar una solución de registro que almacene las entradas de **journal** en un archivo local, mientras que las entradas leídas de los archivos se reenvían a otro sistema de registro y se almacenan en los archivos de registro locales.

14.2. PARÁMETROS DE LA FUNCIÓN DEL SISTEMA DE REGISTRO

En un playbook de Logging System Role, se definen las entradas en el parámetro **logging_inputs**, las salidas en el parámetro **logging_outputs** y las relaciones entre las entradas y salidas en el parámetro **logging_flows**. El rol de sistema de registro procesa estas variables con opciones adicionales para configurar el sistema de registro. También puede habilitar la encriptación.

NOTA

Actualmente, el único sistema de registro disponible en el rol de sistema de registro es **Rsyslog**.

- **logging_inputs** - Lista de entradas para la solución de registro.
  - **name** - Nombre único de la entrada. Se utiliza en la lista de entradas de **logging_flows** y forma parte del nombre del archivo generado de **config**.
  - **type** - Tipo del elemento de entrada. El tipo especifica un tipo de tarea que corresponde a un nombre de directorio en **roles/rsyslog/{tasks,vars}/inputs/**.
    - **basics** - Entradas que configuran las entradas desde el diario **systemd** o el zócalo **unix**.
      - **kernel_message** - Cargar **imklog** si se ajusta a **true**. Por defecto, **false**.
      - **use_imuxsock** - Utilice **imuxsock** en lugar de **imjournal**. Por defecto, **false**.
      - **ratelimit_burst** - Número máximo de mensajes que se pueden emitir dentro de **ratelimit_interval**. Por defecto es **20000** si **use_imuxsock** es falso. Por defecto a **200** si **use_imuxsock** es verdadero.
      - **ratelimit_interval** - Intervalo para evaluar **ratelimit_burst**. Por defecto, 600 segundos si **use_imuxsock** es falso. Por defecto es 0 si **use_imuxsock** es verdadero. 0 indica que la limitación de velocidad está desactivada.
      - **persist_state_interval** - El estado del diario se mantiene cada **value** mensajes. Por defecto es **10**. Sólo es efectivo cuando **use_imuxsock** es falso.
    - **files** - Entradas que configuran las entradas de los archivos locales.
    - **remote** - Entradas que configuran las entradas del otro sistema de registro a través de la red.
  - **state** - Estado del archivo de configuración. **present** o **absent**. Por defecto, **present**.
- **logging_outputs** - Lista de salidas para la solución de registro.
  - **files** - Salidas que configuran las salidas a los archivos locales.
  - **forwards** - Salidas que configuran las salidas a otro sistema de registro.
  - **remote_files** - Salidas que configuran salidas de otro sistema de registro a archivos locales.
- **logging_flows** - Lista de movimientos que definen las relaciones entre **logging_inputs** y **logging_outputs**. La variable **logging_flows** tiene las siguientes claves:
  - **name** - Nombre único del flujo
  - **inputs** - Lista de valores del nombre **logging_inputs**
  - **outputs** - Lista de valores del nombre **logging_outputs**.

Recursos adicionales

- Documentación instalada con el paquete **rhel-system-roles** en **/usr/share/ansible/roles/rhel-system-roles.logging/README.html**

14.3. APLICACIÓN DE UN ROL DE SISTEMA DE REGISTRO LOCAL

Siga estos pasos para preparar y aplicar un playbook de Red Hat Ansible Engine para configurar una solución de registro en un conjunto de máquinas separadas. Cada máquina registrará los registros localmente.

Requisitos previos

- Tiene instalado Red Hat Ansible Engine en el sistema desde el que desea ejecutar el libro de jugadas.

NOTA

No es necesario que tenga instalado Red Hat Ansible Engine en los sistemas en los que desee implementar la solución de registro.

- Tiene el paquete **rhel-system-roles** en el sistema desde el que quiere ejecutar el libro de jugadas.

NOTA

No es necesario tener instalado **rsyslog**, porque el rol de sistema instala **rsyslog** cuando se despliega.

- Tiene un archivo de inventario que enumera los sistemas en los que desea configurar la solución de registro.

Procedimiento

1. Cree un libro de jugadas que defina el rol requerido:
   a. Cree un nuevo archivo YAML y ábralo en un editor de texto, por ejemplo:

```
# vi logging-playbook.yml
```

   b. Inserte el siguiente contenido:

```
---
- name: Deploying basics input and implicit files output
  hosts: all
  roles:
    - linux-system-roles.logging
  vars:
    logging_inputs:
      - name: system_input
        type: basics
    logging_outputs:
      - name: files_output
        type: files
    logging_flows:
      - name: flow1
        inputs: [system_input]
        outputs: [files_output]
```

2. Ejecutar el libro de jugadas en un inventario específico:
   ■

```
# ansible-playbook -i inventory-file /path/to/file/logging-playbook.yml
```

Dónde:

- ***inventory-file*** es el archivo de inventario.
- ***logging-playbook.yml*** es el libro de jugadas que utilizas.

Verificación

1. Pruebe la sintaxis del archivo **/etc/rsyslog.conf**:

```
# rsyslogd -N 1
rsyslogd: version 8.1911.0-6.el8, config validation run (level 1), master config
/etc/rsyslog.conf
rsyslogd: End of config validation run. Bye.
```

2. Compruebe que el sistema envía mensajes al registro:
   a. Envía un mensaje de prueba:

```
# logger test
```

   b. Vea el registro de **/var/log/messages**, por ejemplo:

```
# cat /var/log/messages
Aug  5 13:48:31 hostname root[6778]: test
```

   Donde `*hostname*` es el nombre del host del sistema cliente. Tenga en cuenta que el registro contiene el nombre del usuario que introdujo el comando del registrador, en este caso **root**.

14.4. APLICACIÓN DE UNA SOLUCIÓN DE REGISTRO REMOTO MEDIANTE EL ROL DE SISTEMA DE REGISTRO

Siga estos pasos para preparar y aplicar un libro de jugadas de Red Hat Ansible Engine para configurar una solución de registro remoto. En este libro de jugadas, uno o más clientes toman los registros de **systemd-journal** y los envían a un servidor remoto. El servidor recibe la entrada remota de **remote_rsyslog** y **remote_files** y envía los registros a archivos locales en directorios nombrados por nombres de hosts remotos.

Requisitos previos

- Tiene instalado Red Hat Ansible Engine en el sistema desde el que desea ejecutar el libro de jugadas.

NOTA

No es necesario que tenga instalado Red Hat Ansible Engine en los sistemas en los que desee implementar la solución de registro.

- Tiene el paquete **rhel-system-roles** en el sistema desde el que quiere ejecutar el libro de jugadas.

NOTA

No es necesario tener instalado **rsyslog**, porque el rol de sistema instala **rsyslog** cuando se despliega.

- Tienes al menos dos sistemas:
  - Al menos uno será el servidor de registro.
  - Al menos uno será el cliente de registro.

Procedimiento

1. Cree un libro de jugadas que defina el rol requerido:
   a. Cree un nuevo archivo YAML y ábralo en un editor de texto, por ejemplo:

```
# vi logging-playbook.yml
```

   b. Inserte el siguiente contenido en el archivo:

```
---
- name: Deploying remote input and remote_files output
  hosts: server
  roles:
    - linux-system-roles.logging
  vars:
    logging_inputs:
      - name: remote_udp_input
        type: remote
        udp_ports: [ 601 ]
      - name: remote_tcp_input
        type: remote
        tcp_ports: [ 601 ]
    logging_outputs:
      - name: remote_files_output
        type: remote_files
    logging_flows:
      - name: flow_0
        inputs: [remote_udp_input, remote_tcp_input]
        outputs: [remote_files_output]

- name: Deploying basics input and forwards output
  hosts: clients
  roles:
    - linux-system-roles.logging
  vars:
    logging_inputs:
      - name: basic_input
        type: basics
    logging_outputs:
      - name: forward_output0
        type: forwards
        severity: info
        target: host1.example.com
        udp_port: 601
```

```
      - name: forward_output1
        type: forwards
        facility: mail
        target: host1.example.com
        tcp_port: 601
    logging_flows:
      - name: flows0
        inputs: [basic_input]
        outputs: [forward_output0, forward_output1]

[basic_input]
[forward_output0, forward_output1]
```

Donde ***host1.example.com*** es el servidor de registro.

NOTA

Puede modificar los parámetros del libro de jugadas para adaptarlos a sus necesidades.

AVISO

La solución de registro sólo funciona con los puertos definidos en la política SELinux del sistema servidor o cliente y abiertos en el cortafuegos. La política SELinux por defecto incluye los puertos 601, 514, 6514, 10514 y 20514. Para utilizar un puerto diferente, modifique la política SELinux en los sistemas cliente y servidor . La configuración del cortafuegos a través de los roles del sistema aún no está soportada.

2. Cree un archivo de inventario que enumere sus servidores y clientes:

   a. Cree un nuevo archivo y ábralo en un editor de texto, por ejemplo:

   ```
   # vi inventory.ini
   ```

   b. Inserte el siguiente contenido en el archivo de inventario:

   ```
   [servers]
   server ansible_host=host1.example.com
   [clients]
   client ansible_host=host2.example.com
   ```

   Where: * ***host1.example.com*** is the logging server. * ***host2.example.com*** is the logging client.

3. Ejecute el libro de jugadas en su inventario.

   ```
   # ansible-playbook -i /path/to/file/inventory.ini /path/to/file/_logging-playbook.yml
   ```

   Dónde:

- ***inventory.ini*** es el archivo de inventario.
- ***logging-playbook.yml*** es el libro de jugadas que has creado.

Pasos de verificación

1. Tanto en el sistema cliente como en el servidor, compruebe la sintaxis del archivo **/etc/rsyslog.conf**:

```
# rsyslogd -N 1
rsyslogd: version 8.1911.0-6.el8, config validation run (level 1), master config
/etc/rsyslog.conf
rsyslogd: End of config validation run. Bye.
```

2. Compruebe que el sistema cliente envía mensajes al servidor:
   a. En el sistema cliente, envíe un mensaje de prueba:

```
# logger test
```

   b. En el sistema del servidor, vea el registro **/var/log/messages**, por ejemplo:

```
# cat /var/log/messages
Aug  5 13:48:31 host2.example.com root[6778]: test
```

   Donde ***host2.example.com*** es el nombre del host del sistema cliente. Tenga en cuenta que el registro contiene el nombre del usuario que introdujo el comando del registrador, en este caso **root**.

Recursos adicionales

- Introducción a los roles de sistema de RHEL
- Documentación instalada con el paquete **rhel-system-roles** en **/usr/share/ansible/roles/rhel-system-roles.logging/README.html**
- Artículo de la KB sobre losroles del sistema RHEL

14.5. RECURSOS ADICIONALES

- Introducción a los roles de sistema de RHEL
- Documentación instalada con el paquete **rhel-system-roles** en **/usr/share/ansible/roles/rhel-system-roles.logging/README.html**
- Artículo de la KB sobre losroles del sistema RHEL

CAPÍTULO 15. USO DE PYTHON

15.1. INTRODUCCIÓN A PYTHON

Python es un lenguaje de programación de alto nivel que soporta múltiples paradigmas de programación, como el orientado a objetos, el imperativo, el funcional y el procedimental. Python tiene una semántica dinámica y puede utilizarse para la programación de propósito general.

Con Red Hat Enterprise Linux, muchos paquetes que se instalan en el sistema, como los paquetes que proporcionan herramientas del sistema, herramientas para el análisis de datos o aplicaciones web, están escritos en Python. Para poder utilizar estos paquetes, es necesario tener instalados los paquetes **python**.

15.1.1. Versiones de Python

Existen dos versiones incompatibles de Python, Python 2.x y Python 3.x.

RHEL 8 proporciona las siguientes versiones de Python.

Versión	Paquete a instalar	Ejemplos de comandos	Disponible desde	Ciclo de vida
Python 3.6	**python3**	**python3**, **pip3**	RHEL 8.0	rHEL 8 completo
Python 2.7	**python2**	**python2**, **pip2**	RHEL 8.0	más corto
Python 3.8	**python38**	**python3.8**, **pip3.8**	RHEL 8.2	más corto

Consulte Red Hat Enterprise Linux Life Cycle y Red Hat Enterprise Linux 8 Application Streams Life Cycle para obtener detalles sobre la duración del soporte.

Cada una de las versiones de Python se distribuye en un módulo independiente y, por su diseño, se pueden instalar varios módulos en paralelo en el mismo sistema.

El módulo **python38** no incluye los mismos enlaces a las herramientas del sistema (RPM, DNF, SELinux y otras) que se proporcionan para el módulo **python36**.

IMPORTANTE

Especifica siempre la versión de Python cuando lo instales, lo invoques o interactúes con él. Por ejemplo, utilice **python3** en lugar de **python** en los nombres de paquetes y comandos. Todos los comandos relacionados con Python deben incluir también la versión, por ejemplo, **pip3**, **pip2**, o **pip3.8**.

El comando **python** no versionado(**/usr/bin/python**) no está disponible por defecto en RHEL 8. Puede configurarlo utilizando el comando **alternatives**; para obtener instrucciones, consulte Configuración del Python no versionado. Cualquier cambio manual en **/usr/bin/python**, excepto los cambios realizados con el comando **alternatives**, puede ser sobrescrito en una actualización.

Como administrador del sistema, se recomienda utilizar preferentemente Python 3 por las siguientes razones:

- Python 3 representa la principal dirección de desarrollo del proyecto Python.
- El apoyo a Python 2 en la comunidad upstream finaliza en 2020.
- Las bibliotecas populares de Python están dejando de soportar Python 2 en el upstream.
- Python 2 en Red Hat Enterprise Linux 8 tendrá un ciclo de vida más corto y su objetivo es facilitar a los clientes una transición más suave a **Python 3**.

Para los desarrolladores, Python 3 tiene las siguientes ventajas sobre Python 2:

- Python 3 permite escribir código expresivo, mantenible y correcto con mayor facilidad.
- El código escrito en Python 3 tendrá una mayor longevidad.
- Python 3 tiene nuevas características, incluyendo asyncio, f-strings, desempaquetado avanzado, argumentos de sólo palabra clave, excepciones encadenadas y más.

Sin embargo, el software existente tiende a requerir que **/usr/bin/python** sea Python 2. Por esta razón, no se distribuye ningún paquete **python** por defecto con Red Hat Enterprise Linux 8, y se puede elegir entre usar Python 2 y 3 como **/usr/bin/python**, como se describe en Sección 15.2.5, “Configurar el Python no versionado”.

15.1.2. El paquete interno platform-python

Las herramientas del sistema en Red Hat Enterprise Linux 8 utilizan una versión 3.6 de Python proporcionada por el paquete interno **platform-python**. Red Hat aconseja a los clientes utilizar el paquete **python36** en su lugar.

15.2. INSTALACIÓN Y USO DE PYTHON

AVISO

El uso del comando **python** sin versión para instalar o ejecutar Python no funciona por defecto debido a la ambigüedad. Especifique siempre la versión de Python, o configure la versión por defecto del sistema mediante el comando **alternatives**.

15.2.1. Instalación de Python 3

En Red Hat Enterprise Linux 8, Python 3 se distribuye en las versiones 3.6 y 3.8, proporcionadas por los módulos **python36** y **python38** en el repositorio AppStream.

Procedimiento

- Para instalar Python 3.6 desde el módulo **python36**, ejecute el siguiente comando:

```
# yum install python3
```

El flujo del módulo python36:3.6 se activa automáticamente.

- Para instalar Python 3.8 desde el módulo **python38**, utilice:

```
# yum install python38
```

El flujo del módulo python38:3.8 se activa automáticamente.

Para obtener detalles sobre los módulos en RHEL 8, consulte Instalación, gestión y eliminación de componentes del espacio de usuario.

NOTA

Por diseño, los módulos de RHEL 8 pueden instalarse en paralelo, incluyendo los módulos **python27**, **python36**, y **python38**. Tenga en cuenta que la instalación en paralelo no es compatible con múltiples flujos dentro de un mismo módulo.

Python 3.8 y los paquetes construidos para él pueden instalarse en paralelo con Python 3.6 en el mismo sistema, con la excepción del módulo **mod_wsgi**. Debido a una limitación del servidor HTTP Apache, sólo se puede instalar uno de los paquetes **python3-mod_wsgi** y **python38-mod_wsgi** en un sistema.

Los paquetes con módulos adicionales para Python 3.6 suelen utilizar el prefijo **python3-**; los paquetes para Python 3.8 incluyen el prefijo **python38-**. Incluya siempre el prefijo cuando instale paquetes adicionales de Python, como se muestra en los ejemplos siguientes.

Procedimiento

- Para instalar el módulo **Requests** para Python 3.6, ejecute este comando:

```
# yum install python3-requests
```

- Para instalar la extensión **Cython** en Python 3.8, utilice:

```
# yum install python38-Cython
```

15.2.1.1. Instalación de paquetes adicionales de Python 3 para desarrolladores

Los paquetes adicionales de Python 3.8 para desarrolladores se distribuyen a través del repositorio CodeReady Linux Builder en el módulo **python38-devel**. Este módulo contiene el paquete **python38-pytest** y sus dependencias: los paquetes **pyparsing**, **atomicwrites**, **attrs**, **packaging**, **py**, **more-itertools**, **pluggy**, y **wcwidth**.

IMPORTANTE

El repositorio CodeReady Linux Builder y su contenido no es soportado por Red Hat.

Para instalar paquetes desde el módulo **python38-devel**, siga el siguiente procedimiento.

Procedimiento

- Habilitar el repositorio CodeReady Linux Builder no soportado:

```
# subscription-manager repos --enable codeready-builder-for-rhel-8-x86_64-rpms
```

- Habilite el módulo **python38-devel**:

```
# yum module enable python38-devel
```

- Instale el paquete **python38-pytest**:

```
# yum install python38-pytest
```

Para más información sobre el repositorio de CodeReady Linux Builder, consulte Cómo habilitar y hacer uso del contenido dentro de CodeReady Linux Builder.

15.2.2. Instalación de Python 2

Algunos programas aún no han sido portados completamente a Python 3 y necesitan Python 2 para funcionar. Red Hat Enterprise Linux 8 permite la instalación paralela de Python 3 y Python 2. Si necesita la funcionalidad de Python 2, instale el módulo **python27**, que está disponible en el repositorio de AppStream.

AVISO

Tenga en cuenta que Python 3 es la principal dirección de desarrollo del proyecto Python. El soporte para Python 2 está siendo eliminado gradualmente. El módulo **python27** tiene un periodo de soporte más corto que Red Hat Enterprise Linux 8.

Procedimiento

- Para instalar Python 2.7 desde el módulo **python27**, ejecute este comando:

```
# yum install python2
```

El flujo del módulo python27:2.7 se activa automáticamente.

NOTA

Por diseño, los módulos de RHEL 8 pueden instalarse en paralelo, incluyendo los módulos **python27**, **python36** y **python38**.

Para más detalles sobre los módulos, véase Instalación, gestión y eliminación de componentes del espacio de usuario.

Los paquetes con módulos adicionales para Python 2 suelen utilizar el prefijo **python2-**. Incluya siempre el prefijo cuando instale paquetes adicionales de Python, como se muestra en los ejemplos siguientes.

Procedimiento

- Para instalar el módulo **Requests** para Python 2, ejecute este comando:

```
# yum install python2-requests
```

- Para instalar la extensión **Cython** en Python 2, utilice:

```
# yum install python2-Cython
```

15.2.3. Uso de Python 3

Cuando ejecute el intérprete de Python o los comandos relacionados con Python, especifique siempre la versión.

Procedimiento

- Para ejecutar el intérprete de Python 3.6 o los comandos relacionados, utilice, por ejemplo

```
$ python3
$ python3 -m cython --help
$ pip3 install <package>
```

- Para ejecutar el intérprete de Python 3.8 o los comandos relacionados, utilice, por ejemplo

```
$ python3.8
$ python3.8 -m cython --help
$ pip3.8 install <package>
```

15.2.4. Uso de Python 2

Cuando ejecute el intérprete de Python 2 o comandos relacionados con Python2, especifique siempre la versión.

Procedimiento

- Para ejecutar el intérprete de Python 2 o los comandos relacionados, utilice, por ejemplo

```
$ python2
$ python2 -m cython --help
$ pip2 install <package>
```

15.2.5. Configurar el Python no versionado

Los administradores del sistema pueden configurar el comando no versionado **python**, ubicado en **/usr/bin/python**, utilizando el comando **alternatives**. Tenga en cuenta que el paquete requerido, **python3**, **python38**, o **python2**, necesita ser instalado antes de configurar el comando no versionado a la versión respectiva.

IMPORTANTE

El ejecutable **/usr/bin/python** está controlado por el sistema **alternatives**. Cualquier cambio manual puede ser sobrescrito en una actualización.

Otros comandos relacionados con Python, como **pip3**, no tienen variantes configurables sin versionar.

15.2.5.1. Configurar directamente el comando python no versionado

Para configurar el comando no versionado **python** directamente a una versión seleccionada de Python, utilice este procedimiento.

Procedimiento

- Para configurar el comando **python** no versionado a Python 3.6, ejecute este comando:

```
# alternatives --set python /usr/bin/python3
```

- Para configurar el comando **python** no versionado a Python 3.8, utilice el siguiente comando:

```
# alternatives --set python /usr/bin/python3.8
```

- Para configurar el comando **python** no versionado a Python 2, utilice:

```
# alternativas --set python /usr/bin/python2
```

15.2.5.2. Configurar el comando python no versionado a la versión de Python requerida de forma interactiva

También puede configurar el comando **python** no versionado a la versión de Python requerida de forma interactiva.

Para configurar el comando **python** no versionado de forma interactiva, utilice este procedimiento.

Procedimiento

1. Ejecute el siguiente comando:

```
# alternativas --config python
```

2. Seleccione la versión requerida de la lista proporcionada.
3. Para restablecer esta configuración y eliminar el comando **python** no versionado, ejecute:

```
# alternativas --auto python
```

15.3. MIGRACIÓN DE PYTHON 2 A PYTHON 3

Como desarrollador, es posible que quieras migrar tu antiguo código escrito en Python 2 a Python 3. Para obtener más información sobre cómo migrar grandes bases de código a Python 3, consulta The Conservative Python 3 Porting Guide.

Tenga en cuenta que después de esta migración, el código original de Python 2 se convierte en interpretable por el intérprete de Python 3 y sigue siendo interpretable para el intérprete de Python 2 también.

15.4. EMPAQUETADO DE RPMS DE PYTHON 3

La mayoría de los proyectos de Python utilizan Setuptools para el empaquetado, y definen la información del paquete en el archivo **setup.py**. Para más información sobre el empaquetado de Setuptools, consulte la documentación de Setuptools.

También puedes empaquetar tu proyecto Python en un paquete RPM, que proporciona las siguientes ventajas en comparación con el empaquetado de Setuptools:

- Especificación de las dependencias de un paquete con otros RPM (incluso los que no son de Python)
- Firma criptográfica
  Con la firma criptográfica, el contenido de los paquetes RPM puede ser verificado, integrado y probado con el resto del sistema operativo.

15.4.1. Descripción del archivo SPEC para un paquete Python

Un archivo SPEC contiene instrucciones que la utilidad **rpmbuild** utiliza para construir un RPM. Las instrucciones se incluyen en una serie de secciones. Un archivo SPEC tiene dos partes principales en las que se definen las secciones:

- Preámbulo (contiene una serie de metadatos que se utilizan en el cuerpo)
- Cuerpo (contiene la parte principal de las instrucciones)

Para más información sobre los archivos SPEC, consulte Empaquetado y distribución de software.

Un archivo RPM SPEC para proyectos de Python tiene algunas especificidades en comparación con los archivos RPM SPEC que no son de Python. En particular, el nombre de cualquier paquete RPM de una biblioteca de Python debe incluir siempre el prefijo que determina la versión, por ejemplo, **python3** para Python 3.6 o **python38** para Python 3.8.

En el siguiente archivo SPEC se muestran otros datos específicos **example for the python3-detox package**. Para la descripción de estos detalles, consulte las notas debajo del ejemplo.

```
%global modname detox                                                    (1)

Name:           python3-detox                                            (2)
Version:        0.12
Release:        4%{?dist}
Summary:        Distributing activities of the tox tool
License:        MIT
URL:            https://pypi.io/project/detox
Source0:        https://pypi.io/packages/source/d/%{modname}/%{modname}-%{version}.tar.gz

BuildArch:      noarch

BuildRequires:  python36-devel                                           (3)
BuildRequires:  python3-setuptools
BuildRequires:  python36-rpm-macros
BuildRequires:  python3-six
BuildRequires:  python3-tox
BuildRequires:  python3-py
BuildRequires:  python3-eventlet

%?python_enable_dependency_generator                                     (4)
```

```
%description

Detox is the distributed version of the tox python testing tool. It makes efficient use of multiple CPUs
by running all possible activities in parallel.
Detox has the same options and configuration that tox has, so after installation you can run it in the
same way and with the same options that you use for tox.

   $ detox

%prep
%autosetup -n %{modname}-%{version}

%build
%py3_build                                                    5

%install
%py3_install

%check
%{__python3} setup.py test                                    6

%files -n python3-%{modname}
%doc CHANGELOG
%license LICENSE
%{_bindir}/detox
%{python3_sitelib}/%{modname}/
%{python3_sitelib}/%{modname}-%{version}*

%changelog
...
```

1. La macro **modname** contiene el nombre del proyecto Python. En este ejemplo es **detox**.

2. Cuando se empaqueta un proyecto Python en RPM, el prefijo **python3** siempre debe añadirse al nombre original del proyecto. El nombre original aquí es **detox** y el **name of the RPM** es **python3-detox**.

3. **BuildRequires** especifica qué paquetes son necesarios para construir y probar este paquete. En BuildRequires, incluya siempre los elementos que proporcionan las herramientas necesarias para construir paquetes de Python: **python36-devel** y **python3-setuptools**. El paquete **python36-rpm-macros** es necesario para que los archivos con **/usr/bin/python3** shebangs se cambien automáticamente a **/usr/bin/python3.6**. Para más información, consulte Sección 15.4.4, “Manejo de hashbangs en scripts de Python”.

4. Cada paquete de Python requiere algunos otros paquetes para funcionar correctamente. Dichos paquetes deben especificarse también en el archivo SPEC. Para especificar el **dependencies**, puede utilizar la macro **%python_enable_dependency_generator** para utilizar automáticamente las dependencias definidas en el archivo **setup.py**. Si un paquete tiene dependencias que no se especifican usando Setuptools, especifíquelas dentro de las directivas adicionales **Requires**.

5. Las macros **%py3_build** y **%py3_install** ejecutan los comandos **setup.py build** y **setup.py install**, respectivamente, con argumentos adicionales para especificar las ubicaciones de instalación, el intérprete a utilizar y otros detalles.

6. La sección **check** proporciona una macro que ejecuta la versión correcta de Python. La macro **%{__python3}** contiene una ruta para el intérprete de Python 3, por ejemplo **/usr/bin/python3**. Recomendamos utilizar siempre la macro en lugar de una ruta literal

Recomendamos utilizar siempre la macro en lugar de una ruta literal.

15.4.2. Macros comunes para los RPM de Python 3

En un archivo SPEC, utilice siempre las siguientes macros en lugar de codificar sus valores.

En los nombres de las macros, utilice siempre **python3** o **python2** en lugar de **python** sin versionar. Configure la versión particular de Python 3 en el **BuildRequires** del archivo SPEC a **python36-rpm-macros** o **python38-rpm-macros**.

Macro	Definición normal	Descripción
%{__python3}	/usr/bin/python3	Intérprete de Python 3
%{python3_version}	3.6	La versión completa del intérprete de Python 3.
%{python3_sitelib}	/usr/lib/python3.6/paquetes-sitio	Donde se instalan los módulos de Python puro.
%{python3_sitearch}	/usr/lib64/python3.6/site-packages	Donde se instalan los módulos que contienen extensiones específicas de la arquitectura.
%py3_build		Ejecuta el comando **setup.py build** con argumentos adecuados para un paquete del sistema.
%py3_install		Ejecuta el comando **setup.py install** con argumentos adecuados para un paquete del sistema.

15.4.3. Proporciona automáticamente los RPM de Python

Al empaquetar un proyecto Python, asegúrese de que, si están presentes, los siguientes directorios se incluyan en el RPM resultante:

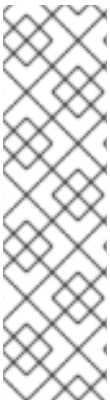
- **.dist-info**
- **.egg-info**
- **.egg-link**

A partir de estos directorios, el proceso de compilación de RPM genera automáticamente los suministros virtuales **pythonX.Ydist**, por ejemplo, **python3.6dist(detox)**. Estos "virtual provides" son utilizados por los paquetes especificados por la macro **%python_enable_dependency_generator**.

15.4.4. Manejo de hashbangs en scripts de Python

En Red Hat Enterprise Linux 8, se espera que los scripts ejecutables de Python usen hashbangs (shebangs) especificando explícitamente al menos la versión principal de Python.

El script **/usr/lib/rpm/redhat/brp-mangle-shebangs** buildroot policy (BRP) se ejecuta automáticamente al construir cualquier paquete RPM, e intenta corregir los hashbangs en todos los archivos ejecutables.



NOTA

El script BRP genera errores cuando encuentra un script Python con un hashbang ambiguo, como por ejemplo

```
#! /usr/bin/python
```

o

```
#! /usr/bin/env python
```

15.4.4.1. Modificación de hashbangs en scripts de Python

Para modificar los hashbangs en los scripts de Python que causan los errores de compilación en el momento de la compilación de RPM, utilice este procedimiento.

Procedimiento

- Aplique el script **pathfix.py** del paquete **platform-python-devel**:

  ```
  # pathfix.py -pn -i %{__python3} PATH...
  ```

  Tenga en cuenta que se pueden especificar varios ***PATHs*** pueden ser especificados. Si a ***PATH*** es un directorio, **pathfix.py** busca recursivamente cualquier script de Python que coincida con el patrón **^[a-zA-Z0-9_] \.py$**, no sólo los que tengan un hashbang ambiguo. Añade este comando a la sección **%prep** o al final de la sección **%install**.

Alternativamente, modifique los scripts de Python empaquetados para que se ajusten al formato esperado. Para este propósito, **pathfix.py** puede ser usado fuera del proceso de construcción del RPM, también. Cuando ejecute **pathfix.py** fuera de una compilación RPM, sustituya ***__python3*** del ejemplo anterior por una ruta para el hashbang, como **/usr/bin/python3**.

Si los scripts de Python empaquetados requieren otra versión que no sea Python 3.6, ajuste los comandos anteriores para incluir la versión respectiva.

15.4.4.2. Cambiar los hashbangs de /usr/bin/python3 en sus paquetes personalizados

Además, los hashbangs en la forma **/usr/bin/python3** son reemplazados por defecto con hashbangs que apuntan a Python desde el paquete **platform-python** utilizado para las herramientas del sistema con Red Hat Enterprise Linux.

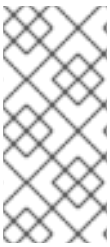
Para cambiar los hashbangs de **/usr/bin/python3** en sus paquetes personalizados para que apunten a una versión de Python instalada desde Application Stream, en la forma **/usr/bin/python3.6**, utilice el siguiente procedimiento.

Procedimiento

- Añada el paquete **python36-rpm-macros** en la sección **BuildRequires** del archivo SPEC incluyendo la siguiente línea:

  ■

```
BuildRequires:  python36-rpm-macros
```



NOTA

Para evitar la comprobación del hashbang y su modificación por el script BRP, utilice la siguiente directiva RPM:

```
%undefine p_mangle_shebangs
```

Si está utilizando otra versión que no sea Python 3.6, ajuste los comandos anteriores para incluir la versión respectiva.

15.4.5. Recursos adicionales

- Para obtener más información sobre el empaquetado de RPM, consulte Empaquetado y distribución de software.

CAPÍTULO 16. USO DEL LENGUAJE DE PROGRAMACIÓN PHP

El Preprocesador de Hipertexto (PHP) es un lenguaje de scripting de propósito general utilizado principalmente para el scripting del lado del servidor, que permite ejecutar el código PHP utilizando un servidor web.

En RHEL 8, el lenguaje de scripting PHP es proporcionado por el módulo **php**, que está disponible en múltiples corrientes (versiones).

Dependiendo de su caso de uso, puede instalar un perfil específico del flujo de módulos seleccionado:

- **common** - El perfil por defecto para el scripting del lado del servidor utilizando un servidor web. Incluye varias extensiones ampliamente utilizadas.
- **minimal** - Este perfil instala sólo la interfaz de línea de comandos para el scripting con PHP sin utilizar un servidor web.
- **devel** - Este perfil incluye paquetes del perfil **common** y paquetes adicionales para fines de desarrollo.

16.1. INSTALACIÓN DEL LENGUAJE DE SCRIPTING PHP

Esta sección describe cómo instalar una versión seleccionada del módulo **php**.

Procedimiento

- Para instalar un flujo de módulos **php** con el perfil por defecto, utilice:

```
# yum module install php<i>stream</i>
```

  Sustituya *stream* por la versión de PHP que desee instalar.

  Por ejemplo, para instalar PHP 7.4:

```
# yum module install php:7.4
```

  El perfil por defecto **common** instala también el paquete **php-fpm**, y preconfigura PHP para su uso con los paquetes **Apache HTTP Server** o **nginx**.

- Para instalar un perfil específico de un flujo de módulos **php**, utilice:

```
# yum module install php<i>stream/profile</i>
```

  Sustituya *stream* por la versión deseada y *profile* por el nombre del perfil que desea instalar.

  Por ejemplo, para instalar PHP 7.4 para utilizarlo sin un servidor web:

```
# yum module install php:7.4/minimal
```

Recursos adicionales

- Si desea actualizar desde una versión anterior de PHP disponible en RHEL 8, consulte Cambiar a una corriente posterior.

- Para obtener más información sobre la gestión de módulos y flujos de RHEL 8, consulte Instalación, gestión y eliminación de componentes del espacio de usuario .

16.2. USO DEL LENGUAJE DE PROGRAMACIÓN PHP CON UN SERVIDOR WEB

16.2.1. Uso de PHP con el servidor HTTP Apache

En RHEL 8, la página **Apache HTTP Server** permite ejecutar PHP como un servidor de procesos FastCGI. El Gestor de Procesos FastCGI (FPM) es un demonio PHP FastCGI alternativo que permite a un sitio web gestionar altas cargas. PHP utiliza FastCGI Process Manager por defecto en RHEL 8.

Esta sección describe cómo ejecutar el código PHP utilizando el servidor de procesos FastCGI.

Requisitos previos

- El lenguaje de programación PHP está instalado en su sistema.
  Véase Sección 16.1, "Instalación del lenguaje de scripting PHP" .

Procedimiento

1. Instale el módulo **httpd**:

```
# yum module install httpd:2.4
```

2. Inicie el **Apache HTTP Server**:

```
# systemctl start httpd
```

   O, si el **Apache HTTP Server** ya está funcionando en su sistema, reinicie el servicio **httpd** después de instalar PHP:

```
# systemctl restart httpd
```

3. Inicie el servicio **php-fpm**:

```
# systemctl start php-fpm
```

4. Opcional: Habilite ambos servicios para que se inicien en el momento del arranque:

```
# systemctl enable php-fpm httpd
```

5. Para obtener información sobre su configuración de PHP, cree el archivo **index.php** con el siguiente contenido en el directorio **/var/www/html/**:

```
echo '<?php phpinfo(); ?>' > /var/www/html/index.php
```

6. Para ejecutar el archivo **index.php**, dirija el navegador a:

```
http://<hostname>/
```

7. Opcional: Ajuste la configuración si tiene requisitos específicos:
   - **/etc/httpd/conf/httpd.conf** - configuración genérica de **httpd**
   - **/etc/httpd/conf.d/php.conf** - Configuración específica de PHP para **httpd**
   - **/usr/lib/systemd/system/httpd.service.d/php-fpm.conf** - por defecto, el servicio **php-fpm** se inicia con **httpd**
   - **/etc/php-fpm.conf** - Configuración principal del FPM
   - **/etc/php-fpm.d/www.conf** - configuración por defecto de la piscina **www**

Ejemplo 16.1. Ejecutar un script PHP "¡Hola, mundo! PHP utilizando el servidor HTTP Apache

1. Cree un directorio **hello** para su proyecto en el directorio **/var/www/html/**:

```
# mkdir hello
```

2. Cree un archivo **hello.php** en el directorio **/var/www/html/hello/** con el siguiente contenido:

```
# <!DOCTYPE html>
<html>
<head>
<title>Hello, World! Page</title>
</head>
<body>
<?php
    echo 'Hello, World!';
?>
</body>
</html>
```

3. Inicie el **Apache HTTP Server**:

```
# systemctl start httpd
```

4. Para ejecutar el archivo **hello.php**, dirija el navegador a:

```
http://<hostname>/hello/hello.php
```

   Como resultado, se muestra una página web con el texto "Hello, World!".

Recursos adicionales

- Configuración del servidor web Apache HTTP

16.2.2. Uso de PHP con el servidor web nginx

Esta sección describe cómo ejecutar código PHP a través del servidor web **nginx**.

Requisitos previos

- El lenguaje de programación PHP está instalado en su sistema.
  Véase Sección 16.1, "Instalación del lenguaje de scripting PHP" .

Procedimiento

1. Instalar un flujo de módulos **nginx**:

   ```
   # yum module install nginx:stream
   ```

   Sustituya *stream* por la versión de **nginx** que desee instalar.

   Por ejemplo, para instalar la versión 1.18 de **nginx**:

   ```
   # yum module install nginx:1.18
   ```

2. Inicie el servidor **nginx**:

   ```
   # systemctl start nginx
   ```

   O, si el servidor **nginx** ya está funcionando en su sistema, reinicie el servicio **nginx** después de instalar PHP:

   ```
   # systemctl restart nginx
   ```

3. Inicie el servicio **php-fpm**:

   ```
   # systemctl start php-fpm
   ```

4. Opcional: Habilite ambos servicios para que se inicien en el momento del arranque:

   ```
   # systemctl enable php-fpm nginx
   ```

5. Para obtener información sobre su configuración de PHP, cree el archivo **index.php** con el siguiente contenido en el directorio **/usr/share/nginx/html/**:

   ```
   echo '<?php phpinfo(); ?>' > /usr/share/nginx/html/index.php
   ```

6. Para ejecutar el archivo **index.php**, dirija el navegador a:

   ```
   http://<hostname>/
   ```

7. Opcional: Ajuste la configuración si tiene requisitos específicos:

   - **/etc/nginx/nginx.conf** - **nginx** configuración principal
   - **/etc/nginx/conf.d/php-fpm.conf** - Configuración de FPM para **nginx**
   - **/etc/php-fpm.conf** - Configuración principal del FPM
   - **/etc/php-fpm.d/www.conf** - configuración por defecto de la piscina **www**

Ejemplo 16.2. Ejecutar un script PHP "¡Hola, mundo! PHP usando el servidor nginx

1. Cree un directorio **hello** para su proyecto en el directorio **/usr/share/nginx/html/**:

```
# mkdir hello
```

2. Cree un archivo **hello.php** en el directorio **/usr/share/nginx/html/hello/** con el siguiente contenido:

```
# <!DOCTYPE html>
<html>
<head>
<title>Hello, World! Page</title>
</head>
<body>
<?php
    echo 'Hello, World!';
?>
</body>
</html>
```

3. Inicie el servidor **nginx**:

```
# systemctl start nginx
```

4. Para ejecutar el archivo **hello.php**, dirija el navegador a:

```
http://<hostname>/hello/hello.php
```

Como resultado, se muestra una página web con el texto "Hello, World!".

16.3. EJECUCIÓN DE UN SCRIPT PHP MEDIANTE LA INTERFAZ DE LÍNEA DE COMANDOS

Un script PHP se ejecuta normalmente mediante un servidor web, pero también puede ejecutarse mediante la interfaz de línea de comandos.

Si desea ejecutar los scripts de **php** utilizando únicamente la línea de comandos, instale el perfil **minimal** de un flujo de módulos **php**.

Consulte Sección 16.1, “Instalación del lenguaje de scripting PHP” para más detalles.

Requisitos previos

- El lenguaje de programación PHP está instalado en su sistema.
  Véase Sección 16.1, “Instalación del lenguaje de scripting PHP” .

Procedimiento

1. En un editor de texto, cree un ***filename*.php** archivo
   Sustituya *filename* por el nombre de su archivo.

2. Ejecute el archivo creado ***filename*.php** desde la línea de comandos:

```
# php filename.php
```

Ejemplo 16.3. Ejecutar un script PHP "¡Hola, mundo! PHP utilizando la interfaz de línea de comandos

1. Cree un archivo **hello.php** con el siguiente contenido utilizando un editor de texto:

```
<?php
    echo 'Hello, World!';
?>
```

2. Ejecute el archivo **hello.php** desde la línea de comandos:

```
# php hola.php
```

Como resultado, se imprime "¡Hola, mundo!".

16.4. RECURSOS ADICIONALES

- **httpd(8)** - La página del manual del servicio **httpd** que contiene la lista completa de sus opciones de línea de comandos.
- **httpd.conf(5)** - La página del manual de configuración de **httpd**, que describe la estructura y la ubicación de los archivos de configuración de **httpd**.
- **nginx(8)** - La página del manual del servidor web **nginx** que contiene la lista completa de sus opciones de línea de comandos y la lista de señales.
- **php-fpm(8)** - La página del manual de PHP FPM que describe la lista completa de sus opciones de línea de comandos y archivos de configuración.

CAPÍTULO 17. USO DE PAQUETES DE IDIOMAS

Langpacks son metapaquetes que instalan paquetes adicionales que contienen traducciones, diccionarios y locales para cada paquete instalado en el sistema.

En un sistema Red Hat Enterprise Linux 8, **langpacks** la instalación se basa en los meta-paquetes del lenguaje **langpacks-<langcode>** y las dependencias débiles de RPM (etiqueta Supplements).

Hay dos requisitos previos para poder utilizar **langpacks** para un idioma seleccionado. Si estos prerrequisitos se cumplen, los metapaquetes de idiomas sacan su langpack para el idioma seleccionado automáticamente en el conjunto de transacciones.

Requisitos previos

- Se ha instalado en el sistema el metapaquete de idiomas **langpacks-<langcode>** para el idioma seleccionado.
  En Red Hat Enterprise Linux 8, los meta paquetes langpacks se instalan automáticamente con la instalación inicial del sistema operativo utilizando el instalador Anaconda, ya que estos paquetes están disponibles en el repositorio in Application Stream.

  Para más información, consulte Sección 17.1, “Comprobación de los idiomas que ofrecen paquetes de idiomas”

- El paquete base, para el que quiere buscar los paquetes locales, ya ha sido instalado en el sistema.

17.1. COMPROBACIÓN DE LOS IDIOMAS QUE OFRECEN PAQUETES DE IDIOMAS

Siga este procedimiento para comprobar qué idiomas ofrecen paquetes de idiomas.

Procedimiento

- Ejecute el siguiente comando:

```
# yum list langpacks-*
```

17.2. TRABAJAR CON PAQUETES DE IDIOMAS BASADOS EN DEPENDENCIAS DÉBILES DE RPM

Esta sección describe múltiples acciones que puede querer realizar al consultar paquetes de idiomas basados en dependencias débiles de RPM, instalando o eliminando el soporte de idiomas.

17.2.1. Listado de soporte de idiomas ya instalados

Para listar el soporte de idiomas ya instalado, utilice este procedimiento.

Procedimiento

- Ejecute el siguiente comando:

```
# yum list installed langpacks*
```

17.2.2. Comprobación de la disponibilidad del soporte lingüístico

Para comprobar si el soporte lingüístico está disponible para cualquier idioma, utilice el siguiente procedimiento.

Procedimiento

- Ejecute el siguiente comando:

```
# yum list available langpacks*
```

17.2.3. Listado de paquetes instalados para un idioma

Para listar qué paquetes se instalan para cualquier idioma, utilice el siguiente procedimiento:

Procedimiento

- Ejecute el siguiente comando:

```
# yum repoquery --whatsupplements langpacks-<locale_code>
```

17.2.4. Instalación del soporte de idiomas

Para añadir un nuevo soporte de idioma, utilice el siguiente procedimiento.

Procedimiento

- Ejecute el siguiente comando:

```
# yum install langpacks-<locale_code>
```

17.2.5. Eliminación del soporte lingüístico

Para eliminar cualquier soporte de idioma instalado, utilice el siguiente procedimiento.

Procedimiento

- Ejecute el siguiente comando:

```
# yum remove langpacks-<locale_code>
```

17.3. AHORRO DE ESPACIO EN DISCO UTILIZANDO GLIBC-LANGPACK-<LOCALE_CODE>

Actualmente, todas las localizaciones se almacenan en el archivo **/usr/lib/locale/locale-archive**, lo que requiere mucho espacio en el disco.

En los sistemas en los que el espacio en disco es un problema crítico, como los contenedores y las imágenes en la nube, o en los que sólo se necesitan unas pocas localizaciones, se pueden utilizar los paquetes glibc locale langpack (**glibc-langpack-<locale_code>**).

Para instalar las localizaciones individualmente, y así obtener una huella de instalación de paquetes más pequeña, utilice el siguiente procedimiento.

Procedimiento

- Ejecute el siguiente comando:

```
# yum install glibc-langpack-<locale_code>
```

Cuando se instala el sistema operativo con Anaconda, se instala **glibc-langpack-<locale_code>** para el idioma que utilizó durante la instalación y también para los idiomas que seleccionó como idiomas adicionales. Tenga en cuenta que **glibc-all-langpacks**, que contiene todas las localizaciones, se instala por defecto, por lo que algunas localizaciones están duplicadas. Si ha instalado **glibc-langpack-<locale_code>** para uno o más idiomas seleccionados, puede eliminar **glibc-all-langpacks** después de la instalación para ahorrar espacio en el disco.

Tenga en cuenta que instalar sólo los paquetes seleccionados de **glibc-langpack-<locale_code>** en lugar de **glibc-all-langpacks** tiene un impacto en el rendimiento en tiempo de ejecución.

NOTA

Si el espacio en disco no es un problema, mantenga todas las locales instaladas utilizando el paquete **glibc-all-langpacks**.

CAPÍTULO 18. INTRODUCCIÓN A TCL/TK

18.1. INTRODUCCIÓN A TCL/TK

Tool command language (Tcl) es un lenguaje de programación dinámico. El intérprete de este lenguaje, junto con la librería C, lo proporciona el paquete **tcl**.

Utilizando **Tcl** emparejado con **Tk** (**Tcl/Tk**) permite crear aplicaciones GUI multiplataforma **Tk** es proporcionada por el paquete **tk**.

Tenga en cuenta que **Tk** puede referirse a cualquiera de los siguientes:

- Un conjunto de herramientas de programación para múltiples lenguajes
- Una librería Tk C disponible para múltiples lenguajes, como C, Ruby, Perl y Python
- Un intérprete de deseos que instancie una consola Tk
- Una extensión de Tk que añade una serie de nuevos comandos a un determinado intérprete de Tcl

Para más información sobre Tcl/Tk, consulte el manual de Tcl/Tk o la página web de documentación de Tcl/Tk.

18.2. CAMBIOS NOTABLES EN TCL/TK 8.6

Red Hat Enterprise Linux 7 utilizado **Tcl/Tk 8.5**. Con Red Hat Enterprise Linux 8, **Tcl/Tk version 8.6** se proporciona en el repositorio del sistema operativo base.

Los principales cambios en **Tcl/Tk 8.6** en comparación con **Tcl/Tk 8.5** son:

- Apoyo a la programación orientada a objetos
- Aplicación de la evaluación sin pilas
- Gestión de excepciones mejorada
- Colección de paquetes de terceros construidos e instalados con Tcl
- Operaciones multihilo habilitadas
- Soporte de scripts con base de datos SQL
- Soporte de red IPv6
- Compresión Zlib integrada
- Procesamiento de la lista
  Están disponibles dos nuevos comandos, **lmap** y **dict map**, que permiten la expresión de transformaciones sobre **Tcl** contenedores.
- Canales apilados por guión
  Están disponibles dos nuevos comandos, **chan push** y **chan pop**, que permiten añadir o eliminar transformaciones hacia o desde los canales de E/S.

Los principales cambios en **Tk** incluyen:

- Soporte de imágenes PNG incorporado
- Ventanas ocupadas
  Está disponible un nuevo comando, **tk busy**, que desactiva la interacción del usuario para una ventana o un widget y muestra el cursor ocupado.
- Nueva interfaz de diálogo de selección de fuentes
- Soporte de texto en ángulo
- Mover cosas en un soporte de lona

Para la lista detallada de cambios entre **Tcl 8.5** y **Tcl 8.6**vea los cambios en Tcl/Tk 8.6.

18.3. MIGRACIÓN A TCL/TK 8.6

Red Hat Enterprise Linux 7 utilizado **Tcl/Tk 8.5**. Con Red Hat Enterprise Linux 8, **Tcl/Tk version 8.6** se proporciona en el repositorio del sistema operativo base.

Esta sección describe la ruta de migración a **Tcl/Tk 8.6** para:

- Los desarrolladores que escriben **Tcl** extensiones o incrustando **Tcl** intérprete en sus aplicaciones
- Tareas de scripting de los usuarios con **Tcl/Tk**

18.3.1. Ruta de migración para desarrolladores de extensiones Tcl

Para que su código sea compatible con **Tcl 8.6**utilice el siguiente procedimiento.

Procedimiento

1. Reescriba el código para utilizar la estructura **interp**. Por ejemplo, si su código dice **interp→errorLine**, reescríbalo para utilizar la siguiente función:

   ```
   Tcl_GetErrorLine(interp)
   ```

   Esto es necesario porque **Tcl 8.6** limita el acceso directo a los miembros de la estructura **interp**.

2. Para que su código sea compatible con ambos **Tcl 8.5** y **Tcl 8.6**utilice el siguiente fragmento de código en un archivo de cabecera de su aplicación o extensión en C que incluya la biblioteca **Tcl** biblioteca:

   ```
   # include <tcl.h>
   # if !defined(Tcl_GetErrorLine)
   # define Tcl_GetErrorLine(interp) (interp→errorLine)
   # endif
   ```

18.3.2. Ruta de migración para los usuarios que programan sus tareas con Tcl/Tk

En **Tcl 8.6**la mayoría de los scripts funcionan igual que con la versión anterior de **Tcl**.

Para migrar su código a **Tcl 8.6**utilice este procedimiento.

Procedimiento

- Cuando escriba un código portable, asegúrese de no utilizar los comandos que ya no se soportan en **Tk 8.6**:

```
tkIconList_Arrange
tkIconList_AutoScan
tkIconList_Btn1
tkIconList_Config
tkIconList_Create
tkIconList_CtrlBtn1
tkIconList_Curselection
tkIconList_DeleteAll
tkIconList_Double1
tkIconList_DrawSelection
tkIconList_FocusIn
tkIconList_FocusOut
tkIconList_Get
tkIconList_Goto
tkIconList_Index
tkIconList_Invoke
tkIconList_KeyPress
tkIconList_Leave1
tkIconList_LeftRight
tkIconList_Motion1
tkIconList_Reset
tkIconList_ReturnKey
tkIconList_See
tkIconList_Select
tkIconList_Selection
tkIconList_ShiftBtn1
tkIconList_UpDown
```

Tenga en cuenta que puede consultar la lista de comandos no compatibles también en el archivo **/usr/share/tk8.6/unsupported.tcl**.