Notas de publicación de Debian 11 (bullseye), ARM EABI

El proyecto de documentación de Debian (https://www.debian.org/doc/)

26 de junio de 2022

Índice general

Capítulo 1

Introducción

Este documento informa a los usuarios de la distribución Debian sobre los cambios más importantes de la versión 11 (nombre en clave «bullseye»).

Las notas de publicación proporcionan la información sobre cómo actualizar de una forma segura desde la versión 10 (nombre en clave «buster») a la versión actual e informan a los usuarios sobre los problemas conocidos que podrían encontrarse durante este proceso.

Puede obtener la versión más reciente de este documento en https://www.debian.org/releases/bullseye/releasenotes.

ATENCIÓN

Tenga en cuenta que es imposible hacer una lista con todos los posibles problemas conocidos y que, por tanto, se ha hecho una selección de los problemas más relevantes basándose en una combinación de la frecuencia con la que pueden aparecer y su impacto en el proceso de actualización.

Tenga en cuenta que solo se da soporte y se documenta la actualización desde la versión anterior de Debian (en este caso, la actualización desde «buster»). Si necesita actualizar su sistema desde una versión más antigua, le sugerimos que primero actualice a la versión buster consultando las ediciones anteriores de las notas de publicación.

1.1. Cómo informar de fallos en este documento

Hemos intentado probar todos los posibles pasos de actualización descritos en este documento y anticipar todos los problemas posibles con los que un usuario podría encontrarse.

En cualquier caso, si piensa que ha encontrado una errata en esta documento, mande un informe de error (en inglés) al sistema de seguimiento de fallos (`https://bugs.debian.org/`) contra el paquete `release-notes`. Puede que desee revisar primero los informes de erratas existentes (`https://bugs.debian.org/release-notes`) para ver si el problema que Vd. ha encontrado ya se ha reportado. Siéntase libre de añadir información adicional a informes de erratas existentes si puede ayudar a mejorar este documento.

Apreciamos y le animamos a que nos envíe informes incluyendo parches a las fuentes del documento. Puede encontrar más información describiendo cómo obtener las fuentes de este documento en Sección 1.3.

1.2. Cómo contribuir con informes de actualización

Agradecemos cualquier información que los usuarios quieran proporcionar relacionada con las actualizaciones desde la versión buster a la versión bullseye. Si está dispuesto a compartir la información, por favor mande un informe de fallo al sistema de seguimiento de fallos (`https://bugs.debian.org/`).

Utilice para el informe el paquete `upgrade-reports` y envíenos el resultado de su actualización. Por favor, comprima cualquier archivo adjunto que incluya (utilizando **gzip**).

Le agradeceríamos que incluyera la siguiente información cuando envíe su informe de actualización:

- El estado de su base de datos de paquetes antes y después de la actualización: la base de datos del estado de `dpkg` (disponible en el archivo `/var/lib/dpkg/status`) y la información del estado de los paquetes de `apt` (disponible en el archivo `/var/lib/apt/extended_states`). Debería realizar una copia de seguridad de esta información antes de hacer la actualización, tal y como se describe en Sección 4.1.1, aunque también puede encontrar copias de seguridad de `/var/lib/dpkg/status` en el directorio `/var/backups`.
- Los registros de la sesión que haya creado al utilizar **script**, tal y como se describe en Sección 4.4.1.
- Sus registros de `apt`, disponibles en el archivo `/var/log/apt/term.log`, o sus registros de **aptitude**, disponibles en el archivo `/var/log/aptitude`.

NOTA

Debería dedicar algún tiempo a revisar y eliminar cualquier información sensible o confidencial de los registros antes de incluirlos dentro de un informe de fallo ya que la información enviada se incluirá en una base de datos pública.

1.3. Fuentes de este documento

Los archivos fuentes de este documento están en formato DocBook XML. La versión HTML se generó utilizando `docbook-xsl` y `xsltproc`. La versión PDF se generó utilizando `dblatex` o `xmlroff`. Los ficheros fuente de las notas de publicación están disponibles en el repositorio de Git del *Proyecto de Documentación de Debian*. Puede utilizar la interfaz web (`https://salsa.debian.org/ddp-team/release-notes/`) para acceder de forma individual a los archivos y consultar los cambios realizados. Consulte las páginas de información de Git del Proyecto de Documentación de Debian (`https://www.debian.org/doc/vcs`) para más información sobre cómo acceder al repositorio de fuentes.

Capítulo 2

Las novedades de Debian 11

Hay más información disponible sobre este tema en el Wiki (`https://wiki.debian.org/NewInBullseye`).

2.1. Arquitecturas soportadas

Las siguientes son las arquitecturas oficialmente soportadas en Debian 11:

- PC de 32 bits (`i386`) y PC de 64 bits (`amd64`)
- ARM de 64 bits (`arm64`)
- ARM EABI (`armel`)
- ARMv7 (EABI hard-float ABI, `armhf`)
- MIPS «little-endian» (`mips64el`)
- MIPS «little-endian» de 64 bits (`mips64el`)
- PowerPC «little-endian» de 64 bits (`ppc64el`)
- IBM System z (`s390x`)

Puede leer más acerca del estado y la información específica de las adaptaciones para su arquitectura en la página web de las adaptaciones de Debian (`https://www.debian.org/ports/`).

2.2. ¿Qué novedades hay en la distribución?

Esta nueva versión de Debian trae de nuevo muchos más programas que su predecesora buster; la distribución incluye más de 11294 paquetes nuevos, para un total de más de 59551 paquetes. La mayor parte de los programas que se distribuyen se han actualizado: más de 42821 paquetes de programas (corresponde a un 72 % de los paquetes en buster). También se han eliminado por varios motivos un número significativo de paquetes (más de 9519, 16 % de los paquetes en buster). No verá ninguna actualización para estos paquetes y se marcarán como «obsoletos» en los programas de gestión de paquetes. Consulte la sección Sección 4.8.

2.2.1. Entornos de escritorio y paquetes conocidos

Debian trae de nuevo varias aplicaciones de escritorio y entornos. Entre otros ahora incluye los entornos de escritorio GNOME 3.38, KDE Plasma 5.20, LXDE 11, LXQt 0.16, MATE 1.24 y Xfce 4.16.

También se han actualizado las aplicaciones de productividad, incluyendo las suites de oficina:

- LibreOffice se ha actualizado a la versión 7.0;
- Calligra se ha actualizado a la versión 3.2.
- GNUcash se ha actualizado a la versión 4.4;

Esta versión, entre muchas otras cosas, incluye las siguientes actualizaciones:

Paquete	Versión en 10 (buster)	Versión en 11 (bullseye)
Apache	2.4.38	2.4.48
BIND Servidor DNS	9.11	9.16
Cryptsetup	2.1	2.3
Dovecot MTA	2.3.4	2.3.13
Emacs	26.1	27.1
Exim servidor de correo predeterminado	4.92	4.94
La colección de compilador GNU como el compilador por omisión	8.3	10.2
GIMP	2.10.8	2.10.22
GnuPG	2.2.12	2.2.27
Inkscape	0.92.4	1.0.2
La biblioteca de C de GNU	2.28	2.31
lighttpd	1.4.53	1.4.59
imagen del núcleo de Linux	serie 4.19	serie 5.10
LLVM/Clang toolchain	6.0.1 y 7.0.1 (por omisión)	9.0.1 y 11.0.1 (por omisión)
MariaDB	10.3	10.5
Nginx	1.14	1.18
OpenJDK	11	11
OpenSSH	7.9p1	8.4p1
Perl	5.28	5.32
PHP	7.3	7.4
Postfix MTA	3.4	3.5
PostgreSQL	11	13
Python 3	3.7.3	3.9.1
Rustc	1.41 (1.34 para `armel`)	1.48
Samba	4.9	4.13
Vim	8.1	8.2

2.2.2. Escaneado e impresión sin controladores

Es muy posible que sea capaz de imprimir con `CUPS` y escanear con `SANE` sin que sea necesario un controlador (a menudo no-libre) para el modelo específico del hardware que utiliza. Especialmente si utiliza dispositivos que entraron en el mercado en los últimos cinco años aproximadamente.

2.2.2.1. CUPS y la impresión sin controlador

Las impresoras modernas que se conectan a la red Ethernet o inalámbrica pueden utilizar la impresión sin controladores (`https://wiki.debian.org/CUPSQuickPrintQueues`), que implementa `CUPS` y `cups-filters`, tal y como se describió en las Notas de publicación de buster (`https://www.debian.org/releases/buster/amd64/release-notes/ch-whats-new.html#driverless-printing`). Debian 11 "bullseye" introduce el nuevo paquete `ipp-usb`, que está recomendado por `cups-daemon` y utiliza el nuevo protocolo independiente de fabricante IPP-sobre-USB (`https://wiki.debian.org/CUPSDriverlessPrinting#ippoverusb`) incluido en muchas impresoras modernas. Esto permite que el dispositivo USB se comporte como un dispositivo de red, extendiendo la impresión sin controlador a impresoras conectadas por USB. Los detalles específicos se describen en el wiki (`https://wiki.debian.org/CUPSDriverlessPrinting#ipp-usb`).

El archivo de servicio de systemd incluído en el paquete `ipp-usb` inicia el demonio `ipp-usb` cuando se conecta una impresora USB, haciendo que sea posible imprimir en ésta. El paquete `cups-browsed` debería configurarse por omisión para utilizarlo automáticamente o se puede configurar manualmente con una cola de impresión local sin controladores (`https://wiki.debian.org/SystemPrinting`).

2.2.2.2. SANE y el escaneado sin controladores

La infraestructura oficial para el uso de `SANE` sin controladores se ofrece por `sane-escl` en `libsane1`. `sane-airscan` es un sistema de uso sin controladores, desarrollado de forma independiente. Ambos servicios entiende el protocolo eSCL (`https://wiki.debian.org/SaneOverNetwork#escl`) pero

`sane-airscan` también utiliza el protocolo WSD (`https://wiki.debian.org/SaneOverNetwork#wsd`). Los usuarios deberían considerar instalar ambos servicios en sus sistemas.

`eSCL` y `WSD` son protocolos de red. Por tanto funcionarán sobre una conexión USB si el dispositivo es del tipo `IPP-sobre-USB` (como se describe anteriormente). Tenga en cuenta que `libsane1` recomienda el paquete `ipp-usb`. Esto permite que el dispositivo adecuado se configure automáticamente utilizando el sistema sin controladores cuando se conecta a un puerto USB.

2.2.3. Nueva orden genérica «open»

Se incluye en el sistema una nueva orden **open** que es un alias de conveniencia a la orden **xdg-open** (por omisión) o a **run-mailcap**. Este alias se gestiona por el sistema update-alternatives(1) (`https://manpages.debian.org//bullseye/dpkg/update-alternatives.1.html`). Esta orden se puede utilizar de forma interactiva en la línea de órdenes para abrir archivos con su aplicación por omisión, que puede ser un programa gráfico cuando esté disponible.

2.2.4. Grupos de control v2

Systemd utiliza por omisión en bullseye los grupos de control v2 (cgroupv2), lo que ofrece una jerarquía de control de recursos unificada. Dispone de parámetros de línea de órdenes del núcleo para volver a activar la versión antigua de cgroups si fuera necesario. Para más información consulte las notas para OpenStack en la sección Sección 5.1.8.

2.2.5. Registro persistente de systemd

Systemd en bullseye activa la funcionalidad de registro persistente por omisión, y guarda los archivos en `/var/log/journal/`. Para conocer los detalles puede consultar systemd-journald.service(8) (`https://manpages.debian.org//bullseye/systemd/systemd-journald.service.8.html`). Tenga en cuenta que en Debian los usuarios del grupo `adm` pueden leer este registro, además del grupo por omisión `systemd-journal`.

Esta configuración no debería interferir con ningún demonio de registro tradicional como pueda ser `rsyslog`. Aquellos usuarios que no dependan de funcionalidades especiales de este tipo de servicios pueden querer desinstalarlo y empezar a utilizar sólo los registros de systemd.

2.2.6. Nuevo método de entrada Fcitx 5

Fcitx 5 es un método de entrada para chino, japonés, coreano y muchos otros idiomas. Es el sucesor del popular método Fcitx 4 que estaba disponible en buster. Esta nueva versión proporciona soporte de Wayland y tiene un mejor soporte de complementos. Puede encontrar más información, incluyendo la guía de migración en el wiki (`https://wiki.debian.org/I18n/Fcitx5`).

2.2.7. Noticias de la mezcla Debian Med

El grupo Debian Med ha tomado parte en la lucha contra el `COVID-19` empaquetando programas utilizados para investigar y secuenciar el virus y para luchar contra la pandemia con herramientas utilizadas por los epidemiólogos. Este esfuerzo continuará en el siguiente ciclo de publicación enfocando el trabajo en herramientas de aprendizaje artificial que se utilizan en ambos campos.

Además de añadir nuevos paquetes en el campo de las ciencias naturales y la medicina, muchos más paquetes se benefician ahora de las funcionalidades de la Integración Continua.

Un abanico de aplicaciones para entornos de misión crítica se benefician de la introducción de SIMD Everywhere (`https://wiki.debian.org/SIMDEverywhere`). Esta librería permite que los paquetes estén disponibles en más plataformas hardware para las que Debian ofrece soporte (fundamentalmente en `arm64`) mientras que mantienen los beneficios de rendimiento que ofrecen los procesadores con extensiones de vectores, como por ejemplo `AVX` en `amd64`, o `NEON` en `arm64`.

Para instalar paquetes mantenidos por el grupo Debian Med, instale los paquetes que comienzan por `med-*`, que están en la versión 3.6.x para Debian bullseye. Puede consultar en las páginas de las tareas de Debian Med (`http://blends.debian.org/med/tasks`) la amplia variedad de programas biológicos y médicos disponible en Debian.

2.2.8. Kernel support for exFAT

bullseye is the first release providing a Linux kernel which has support for the exFAT filesystem, and defaults to using it for mounting exFAT filesystems. Consequently it's no longer required to use the filesystem-in-userspace implementation provided via the `exfat-fuse` package. If you would like to continue to use the filesystem-in-userspace implementation, you need to invoke the **mount.exfat-fuse** helper directly when mounting an exFAT filesystem.

Tools for creating and checking an exFAT filesystem are provided in the `exfatprogs` package by the authors of the Linux kernel exFAT implementation. The independent implementation of those tools provided via the existing `exfat-utils` package is still available, but cannot be co-installed with the new implementation. It's recommended to migrate to the `exfatprogs` package, though you must take care of command options, which are most likely incompatible.

2.2.9. Improved man page translations

The manual pages for several projects such as systemd, util-linux, OpenSSH, and Mutt in a number of languages, including French, Spanish, and Macedonian, have been substantially improved. To benefit from this, please install `manpages-`*`xx`* (where *`xx`* is the code for your preferred natural language).

During the lifetime of the bullseye release, backports of further translation improvements will be provided via the `backports` archive.

2.2.10. Improved support for alternative init systems

The default init system in Debian is `systemd`. In bullseye, a number of alternative init systems are supported (such as System-V-style init and OpenRC), and most desktop environments now work well on systems running alternative inits. Details on how to switch init system (and where to get help with issues related to running inits other than systemd) are available on the Debian wiki (`https://wiki.debian.org/Init`).

Capítulo 3

Sistema de instalación

El instalador de Debian («Debian Installer») es el sistema oficial de instalación de Debian. Éste ofrece varios métodos de instalación. Los métodos disponibles para la instalación dependerán de su arquitectura.

Puede encontrar las imágenes binarias del instalador de bullseye junto con la «Guía de instalación» en la página web de Debian (`https://www.debian.org/releases/bullseye/debian-installer/`).

La «Guía de instalación» también se incluye en el primer medio de los conjuntos de DVD (CD/Blu-ray) oficiales de Debian, en:

```
/doc/install/manual/idioma/index.html
```

Quizás también quiera consultar la página de fallos (`https://www.debian.org/releases/bullseye/debian-installer/index#errata`) conocidos del instalador de Debian.

3.1. Novedades del sistema de instalación

Se ha realizado mucho desarrollo en el instalador de Debian desde su primera versión oficial en Debian 10, dando como resultado una mejora en el soporte de hardware y algunas funcionalidades nuevas muy interesantes.

Si está interesado en un resumen de los cambios detallados desde buster, consulte los anuncios de publicación de las versiones beta y RC de bullseye disponibles en el histórico de noticias (`https://www.debian.org/devel/debian-installer/News/`) del instalador de Debian.

3.1.1. Help with installation of firmware

More and more, peripheral devices require firmware to be loaded as part of the hardware initialization. To help deal with this problem, the installer has a new feature. If some of the installed hardware requires firmware files to be installed, the installer will try to add them to the system, based on a mapping from hardware ID to firmware file names.

This new functionality is restricted to the unofficial installer images with firmware included (see https://www.debian.org/releases/bullseye/debian-installer/#firmware_nonfree (`https://www.debian.org/releases/bullseye/debian-installer/#firmware_nonfree`)). The firmware is usually not DFSG compliant, so it is not possible to distribute it in Debian's main repository.

If you experience problems related to (missing) firmware, please read the dedicated chapter of the installation-guide (`https://www.debian.org/releases/bullseye/amd64/ch06s04#completing-instal`

3.1.2. Instalación automatizada

Some changes also imply changes in the support in the installer for automated installation using preconfiguration files. This means that if you have existing preconfiguration files that worked with the buster installer, you cannot expect these to work with the new installer without modification.

La «Guía de Instalación» (`https://www.debian.org/releases/bullseye/installmanual`) tiene un apéndice separado que incluye extensa documentación sobre cómo utilizar la preconfiguración.

3.2. Imágenes para contenedores y máquinas virtuales

Las imágenes multi-arquitectura de Debian bullseye están disponibles en Docker Hub (`https://hub.docker.com/_/debian`). Además de las imágenes estándar, existe una variante "slim" ("delgada", N. del T.) que reduce el uso en disco.

Las imágenes virtuales para el gestor de maquinas virtuales Hashicorp Vagrant están publicadas en Vagrant Cloud (`https://app.vagrantup.com/debian`).

Capítulo 4

Actualizaciones desde Debian 10 (buster)

4.1. Prepararse para la actualización

Le sugerimos que antes de actualizar lea también la información en Capítulo 5. Ese capítulo cubre problemas que se pueden dar y que no están directamente relacionados con el proceso de actualización, pero que aún así podría ser importante conocer antes de empezar.

4.1.1. Haga copias de seguridad de sus datos e información de configuración

Es muy recomendable realizar una copia de seguridad completa o al menos una de los datos o información de configuración que no pueda permitirse perder antes de actualizar su sistema. Las herramientas y el proceso de actualización son bastante fiables, pero un fallo de hardware a mitad de una actualización podría resultar en un sistema muy dañado.

Los elementos principales que debería querer salvaguardar son los contenidos de `/etc`, `/var/lib/dpkg`, `/var/lib/apt/extended_states` y la salida de «`dpkg --get-selections "*"`» (las comillas son importantes). Si utiliza **aptitude** para gestionar los paquetes en su sistema, también querrá hacer una copia de seguridad de `/var/lib/aptitude/pkgstates`.

El proceso de actualización no modifica nada dentro del directorio `/home`. Algunas aplicaciones (como es el caso de algunas partes del conjunto de aplicaciones Mozilla y el de los entornos de escritorio de KDE y GNOME) sí sobreescribirán la configuración del usuario con los nuevos valores por omisión cuando el usuario arranque una nueva versión de la aplicación. Como medida preventiva quizás desee realizar una copia de seguridad de los directorios y archivos ocultos («dotfiles», archivos que comienzan por punto, N. del T.) en los directorios personales de los usuarios. Esta copia de seguridad le será útil para restaurar o recrear la configuración previa a la actualización. Quizás quiera también avisar a los usuarios de este asunto.

Cualquier operación de instalación de paquetes debe ser ejecutada con privilegios de superusuario, bien accediendo al sistema como `root` o usando los programas **su** o **sudo** para obtener los derechos de acceso necesarios.

La actualización tiene unas cuantas condiciones previas, así que debería revisarlas antes de ponerse a ello.

4.1.2. Informar a los usuarios anticipadamente

Es aconsejable informar a los usuarios con antelación de cualquier actualización que esté planeando realizar, aunque los usuarios que accedan al sistema mediante **ssh** no deberían apenas notar nada durante la actualización, y deberían poder seguir trabajando.

Si desea tomar precauciones adicionales, haga una copia de seguridad, o desmonte la partición `/home` antes de actualizar.

Tendrá que hacer una actualización del núcleo cuando se actualice a bullseye, por lo que será necesario reiniciar el sistema. Esto se realizará habitualmente una vez la actualización haya terminado.

4.1.3. Prepararse para la indisponibilidad de servicios

Es posible que existan servicios ofrecidos por el sistema que están asociados a paquetes incluidos en el proceso de instalación. Si esto sucede, ha de tener en cuenta que los servicios se interrumpirán mientras los paquete asociados se están actualizando o están siendo reemplazados y configurados. El servicio no estará disponible durante este tiempo.

El tiempo exacto de indisponibilidad para estos servicios dependerá del número de paquetes que se están actualizando en el sistema, y también incluye el tiempo que el administrador dedica a responder a las preguntas de configuración de las distintas actualizaciones de paquetes (si las hubiera). Tenga en cuenta que si el proceso de actualización se hace de forma desatendida y el sistema realiza alguna pregunta durante éste hay una alta probabilidad de que los servicios no estén disponibles [1] durante un periodo de tiempo significativo.

Si el sistema que está Vd. actualizando ofrece servicios críticos para sus usuarios o para la red [2], puede reducir el tiempo de disponibilidad si realiza una actualización mínima del sistema como se describe en Sección 4.4.4, seguido de una actualización del núcleo y un reinicio, y después una actualización de los paquetes asociados con sus servicios críticos. Actualice estos paquetes antes de hacer la actualización completa como se describe en Sección 4.4.5. De esta forma puede asegurarse que estos servicios críticos están ejecutándose y disponibles durante todo el proceso de actualización, reduciendo su indisponibilidad.

4.1.4. Prepararse para la recuperación

Aunque Debian intenta garantizar que el sistema es arrancable en todo momento, siempre hay una posibilidad de que experimente problemas al reiniciar el sistema tras la instalación. Muchos de los problemas conocidos se describen tanto en este capítulo como en los siguientes de estas notas de publicación.

Por esta misma razón tiene sentido asegurarse de que es capaz de recuperar el sistema en el caso que este no pudiera reiniciarse o, para aquellos sistemas gestionados de forma remota, no pudiera arrancar correctamente la configuración de red.

Si está actualizando de forma remota a través de un enlace con **ssh** es altamente recomendable que tome las debidas precauciones para poder acceder al servidor a través de un terminal serie remoto. Existe la posibilidad de que tras actualizar el núcleo y reiniciar tenga que arreglar la configuración del sistema a través de una consola remota. Igualmente, es posible que tenga que recuperar con una consola local en caso de que el sistema se reinicie accidentalmente a la mitad de la actualización.

Para recuperaciones de emergencia generalmente recomendamos la utlización del *modo de rescate* del Instalador de Debian de bullseye. La ventaja en el caso de utilizar el instalador es que podrá encontrar, de entre los distintos métodos de instalación, el más apropiado para su situación. Si desea más información, consulte la sección “Recuperar un sistema roto” en el capítulo octavo de la Guía de instalación (`https://www.debian.org/releases/bullseye/installmanual`) y las PUF del Instalador de Debian (`http://wiki.debian.org/DebianInstaller/FAQ`).

Necesitará un mecanismo alternativo para arrancar su sistema y poder acceder al mismo y repararlo si esto fallara. Una opción es utilizar una imagen especial de rescate o una imagen de instalación «viva» (`https://www.debian.org/CD/live/`) («live CD», N. del T.). Una vez haya arrancado con cualquiera de éstos debería poder montar su sistema de archivos raíz y utilizar **chroot** para acceder a éste, investigar y solucionar el problema.

4.1.4.1. Intérprete de línea de órdenes de depuración durante el arranque con initrd

El paquete `initramfs-tools` incluye un intérprete de órdenes de depuración[3] en los «initrds» que genera. Por ejemplo, si el initrd es incapaz de montar su sistema de archivos raíz Vd. accederá a este sistema de depuración. En este sistema podrá utilizar algunas órdenes básicas que pueden ayudarle a trazar el problema y quizás incluso arreglarlo.

Algunas de las cosas básicas a comprobar son: la existencia de los archivos de dispositivos correctos en `/dev`, los módulos cargados (`cat /proc/modules`), y la salida de **dmesg** para ver si se producen

[1] Si la prioridad de debconf se fija al valor «muy alto» no se le realizarán preguntas de configuración, pero los servicios que dependen de las respuestas por omisión pueden no arrancar si las respuestas por omisión no aplican a su sistema.

[2] Por ejemplo: servicios DNS o DHCP, especialmente si no existe ninguna redundancia o mecanismo de alta disponibilidad. En el caso de DHCP los usuarios pueden quedarse desconectados de la red si el tiempo de mantenimiento de las direcciones es inferior al tiempo que tarda el proceso de actualización en completarse.

[3] Esta funcionalidad puede deshabilitarse si añade el parámetro `panic=0` dentro de los parámetros del arranque.

errores al cargar los controladores de dispositivos. La salida de **dmesg** también muestra qué archivos de dispositivos se han asignado a qué discos, debería comparar esa información con la salida de `echo $ROOT` para asegurarse que el sistema de archivos está en el dispositivo que esperaba.

En el caso de que arregle el problema puede escribir `exit` para salir del entorno de depuración y continuar el proceso de arranque a partir del punto que falló. Por supuesto, tendrá que arreglar el problema subyacente y regenerar el «initrd» para que no vuelva a fallar en el siguiente arranque.

4.1.4.2. Intérprete de línea de órdenes de depuración durante el arranque con systemd

En el caso de que falle el arranque con systemd, aún es posible obtener una interfaz de línea de órdenes para depuración como «root» cambiando la línea de órdenes del núcleo. Si el arranque básico funciona, pero algunos servicios no llegan a iniciarse, puede ser útil añadir a los parámetros del núcleo la opción `systemd.unit=rescue.target`.

En cualquier otro caso, el parámetro del núcleo `systemd.unit=emergency.target` le proporcionará un intérprete de órdenes como usuario «root» en el primer momento en que sea posible. Sin embargo, esto se hace antes de que el sistema de archivos raíz se monte con permisos de lectura y escritura. Puede hacerlo manualmente con:

```
# mount -o remount,rw /
```

Puede encontrar más información de la depuración de un sistema de arranque con problemas bajo systemd en el artículo Diagnosticando problemas de arranque (`https://freedesktop.org/wiki/Software/systemd/Debugging/`).

4.1.5. Preparar un entorno seguro para la actualización

> IMPORTANTE
>
> Si está utilizando algún tipo de servicio de VPN (como pueda ser `tinc`) tenga en cuenta que estos pueden no estar disponibles durante el proceso de actualización. Para más información consulte Sección 4.1.3.

Para poder tener un margen de seguridad mayor cuando actualiza de forma remota le sugerimos que realice su proceso de actualización en una consola virtual como la que ofrece el programa **screen**, lo que permite una reconexión segura y asegura que el proceso de actualización no se interrumpe aunque falle el proceso de conexión remota.

Los usuarios del demonio watchdog daemon que ofrece el paquete `micro-evtd` deberían parar el demonio y deshabilitar el temporizador antes de la actualización, para evitar un reinicio espúreo a mitad del proceso de actualización.

```
# service micro-evtd stop
# /usr/sbin/microapl -a system_set_watchdog off
```

4.2. Comenzar de un Debian "puro"

El proceso de actualización descrito en este capítulo ha sido diseñado para sistemas Debian estable "puros". APT controla qué se instalará en su sistema. Si su configuración de APT menciona fuentes adicionales además de buster o si tiene paquetes instalados de otras versiones o de terceros, debería eliminar estos elementos si quiere asegurarse de tener un proceso de actualización fiable.

El archivo principal de configuración que APT utiliza para decidir desde qué fuentes debería descargar paquetes es `/etc/apt/sources.list`, pero también puede utilizar archivos en el directorio `/etc/apt/sources.list.d/`. Para más detalles puede consultar sources.list(5) (`https://manpages.debian.org//bullseye/apt/sources.list.5.html`). Si su sistema utiliza distintos archivos de fuentes debe asegurarse que son consistentes.

4.2.1. Actualización a Debian 10 (buster)

No se proporciona soporte a las actualizaciones directas de versiones de Debian más antiguas que 10 (buster). Puede mostrar su versión de Debian ejecutando:

```
$ cat /etc/debian_version
```

Por favor, siga las instrucciones en las Notas de publicación para Debian 10 (`https://www.debian.org/releases/buster/releasenotes`) para actualizarse primero a Debian 10.

4.2.2. Eliminar paquetes que no son de Debian

A continuación se muestran dos métodos para encontrar paquetes instalados que no son parte de Debian, utilizando bien el programa **aptitude** o el programa **apt-forktracer**. Tenga en cuenta que ninguno de los dos es 100 % exacto (p.ej. el ejemplo con aptitude listará paquetes que en algún momento se ofrecieron en Debian pero que ahora no se ofrecen, como los antiguos paquetes del núcleo).

```
$ aptitude search '?narrow(?installed, ?not(?origin(Debian)))'
$ apt-forktracer | sort
```

4.2.3. Actualización a la siguiente subversión publicada

El procedimiento aquí descrito supone que su sistema se ha actualizado a la última revisión de buster. Debe seguir las instrucciones descritas en Sección A.1 si su sistema no está actualizado o no está seguro de que lo esté.

4.2.4. Preparar la base de datos de paquetes

Debería asegurarse que la base de datos de paquetes está lista antes de proceder con la actualización. Si utiliza algún otro gestor de paquetes como `aptitude` o `synaptic`, es necesario que revise si existe alguna acción pendiente en éstos. El procedimiento de actualización puede verse afectado negativamente si algún paquete está marcado para eliminarse o actualizarse. Tenga en cuenta que solo podrá corregir esto si sus archivos de fuentes APT aún apunta a *buster* y no a *stable* o *bullseye*, consulte Sección A.2.

4.2.5. Eliminar paquetes obsoletos

Es una buena idea eliminar los paquetes obsoletos de su sistema antes de actualizar. Estos paquetes pueden introducir complicaciones durante el proceso de actualización, y pueden introducir problemas de seguridad dado que ya no se mantienen.

4.2.6. Limpieza de restos de archivos de configuración

Una actualización anterior puede haber dejado copias sin utilizar de ficheros de configuración, versiones antiguas de ficheros de configuración, versiones suministradas por los desarrolladores del paquete, etc. Eliminar restos de actualizaciones antiguas puede ayudar a evitar confusiones. Puede encontrar estos restos ejecutando:

```
# find /etc -name '*.dpkg-*' -o -name '*.ucf-*' -o -name '*.merge-error'
```

4.2.7. La sección de seguridad

El formato de las líneas de fuentes APT que referencian a los repositorios de seguridad ha cambiado ligeramente junto con la version de publicación. Se ha pasado del nombre anterior `buster/updates` a `bullseye-security`. Para más información consulte Sección 5.1.2.

4.2.8. La sección "proposed-updates"

Antes de actualizar el sistema debería eliminar la sección `proposed-updates` en sus archivos de fuentes de APT si la tiene listada. Esta medida de precaución reducirá la posibilidad de que se produzcan conflictos.

4.2.9. Fuentes no oficiales

Debe tener en cuenta que si tiene paquetes en el sistema que no sean de Debian es posible que estos se eliminen durante la actualización debido a dependencias que entren en conflicto. Si el paquete se instaló después de añadir un repositorio de paquetes extra en sus archivos de fuentes APT debería asegurarse de que ese repositorio también ofrece paquetes compilados para bullseye y cambiar la línea de la fuente al mismo tiempo que cambia otras líneas de las fuentes de los paquetes Debian.

Algunos usuarios tienen versiones "más nuevas" de paquetes que *sí* están en Debian a través de recompilaciones *no oficiales* («backports», N. del T.) que están instaladas en su sistema buster. Es muy probable que estos paquetes causen problemas durante la actualización y que den lugar a conflictos de archivos[4]. Puede encontrar más información sobre los conflictos de archivos y su resolución en la sección Sección 4.5.

4.2.10. Desactivar el bloqueo de APT

Si ha configurado APT para que instale ciertos paquetes de una distribución distinta de la estable, por ejemplo la distribución "testing" ("en pruebas", N. del T.), puede ser que haya cambiado la configuración de bloqueo (o *pinning*) de APT (almacenada en `/etc/apt/preferences` y `/etc/apt/preferences.d/`) para permitir que se actualicen paquetes con versiones más recientes que en la distribución estable. Puede encontrar más información sobre el bloqueo de APT en apt_preferences(5) (`https://manpages.debian.org//bullseye/apt/apt_preferences.5.en.html`)."

4.2.11. Verificar el estado de los paquetes

Independientemente del método que se use para actualizar, se recomienda que compruebe el estado de todos los paquetes primero, y que verifique que todos los paquetes se encuentran en un estado actualizable. La siguiente orden mostrará cualquier paquete que se haya quedado a medio instalar (estado *Half-Installed*) o en los que haya fallado la configuración (estado *Failed-Config*), así como los que tengan cualquier estado de error.

```
# dpkg --audit
```

También puede inspeccionar el estado de todos los paquetes de su sistema usando **aptitude** o con órdenes tales como:

```
# dpkg -l | pager
```

o

```
# dpkg --get-selections "*" > ~/curr-pkgs.txt
```

Es deseable eliminar cualquier paquete retenido (paquete en estado «hold», N. del T.) antes de actualizar. El proceso fallará si un paquete esencial para la actualización está bloqueado.

Tenga en cuenta que **aptitude** utiliza un método para registrar los paquetes retenidos distinto del que utilizan **apt** y **dselect**. Puede utilizar la siguiente orden para identificar los paquetes que están retenidos en **aptitude**:

```
# aptitude search "~ahold"
```

[4] El sistema de gestión de paquetes no permite por regla general que un paquete elimine o reemplace un archivo que pertenezca a otro paquete a menos que se haya indicado que el nuevo paquete reemplaza al antiguo.

Si quiere comprobar los paquetes que tiene retenidos con **apt** debería utilizar:

```
# dpkg --get-selections | grep 'hold$'
```

Si ha cambiado y recompilado un paquete de forma local, y no le ha cambiado el nombre o marcado con una época («epoch», N. del T.) en la versión, debería retenerlo (ponerlo en *hold*) para evitar que se actualice.

Se puede cambiar el estado de un paquete retenido ("hold") para que lo tengan en cuenta **apt** con la siguiente orden:

```
# echo nombre_del_paquete hold | dpkg --set-selections
```

Cambie `hold` por `install` para borrar la marca del paquete y que este deje de estar retenido.

Si hay algo que debe arreglar es mejor que se asegure de que sus archivos de fuentes APT aún incluyen referencias a buster tal y como se explica en Sección A.2.

4.3. Preparar las fuentes de orígenes para APT

Antes de comenzar la actualización, debe reconfigurar las listas de fuentes de APT (`/etc/apt/sources.list` y los archivos bajo `/etc/apt/sources.list.d/`) para añadir las fuentes de `bullseye` y habitualmente para eliminar las fuentes de `buster`.

APT tomará en consideración todos los paquetes que pueda encontrar mediante una línea que empiece por "`deb`", e instalará el paquete con el mayor número de versión, dando prioridad a las líneas que aparezcan primero. En el caso de utilizar distintos repositorios de paquetes, habitualmente se indicará primero el disco duro local, luego los CD-ROM, y por último las réplicas remotas.

Una versión se puede designar tanto por su nombre en clave (por ejemplo `buster`, `bullseye`) como por su nombre de estado (esto es, `oldstable`, `stable`, `testing`, `unstable`). Referirse a la distribución por su nombre en clave tiene la ventaja de que nunca se sorprenderá si se produce una nueva versión y por esa razón es el caso que aquí se describe. Esto significa que va a tener que estar atento a los anuncios de nuevas versiones. Sin embargo, si utiliza el nombre del estado verá un número muy elevado de actualizaciones de paquetes en el mismo momento en el que la publicación de una nueva versión se haya realizado.

Debian ofrece dos listas de distribución de avisos que le permitirán mantenerse al día de la información relevante relacionada con las publicaciones de Debian:

- Si se suscribe a la lista de distribución de avisos de Debian (`https://lists.debian.org/debian-announce/`), recibirá una notificación cada vez que se publique una nueva versión en Debian. Como por ejemplo cuando `bullseye` cambie de ser, p.ej., `testing` a `stable`.

- Si se subscribe a la lista de distribución de avisos de seguridad de Debian (`https://lists.debian.org/debian-security-announce/`), recibirá una notificación cada vez que Debian publique un aviso de seguridad.

4.3.1. Añadir fuentes en Internet para APT

La configuración por omisión en las nuevas instalaciones es que APT utilice el servicio APT CDN de Debian, que debería asegurarse que los paquetes se descargan automáticamente del servidor más cercano desde el punto de vista de red. Al ser un servicio relativamente nuevo, las instalaciones más antiguas pueden tener una configuración que aún diriga a los servidores principales en Internet de Debian o a una de las réplicas. Se le recomienda que cambie su configuración para utilizar el servicio CDN en su configuración de APT si no lo ha hecho aún.

Para utilizar el servicio CDN, añada una línea como ésta a su configuración de APT (se presupone que está utilizando `main` y `contrib`):

```
deb http://deb.debian.org/debian bullseye main contrib
```

Tras añadir sus nuevas fuentes, desactive las líneas "deb", colocando el símbolo de sostenido (#) delante de ellas.

Sin embargo, si obtiene mejores resultados utilizando una réplica específica que es cerca a su ubicación, esta opción aún sigue estando disponible.

Encontrará la lista de direcciones de las réplicas de Debian en https://www.debian.org/distrib/ftplist (busque en la sección "Lista de completa de sitios de réplica").

Por ejemplo, suponga que su réplica más cercana es http://mirrors.kernel.org/. Si observa su contenido mediante un navegador web, comprobará que los directorios principales están organizados así:

```
http://mirrors.kernel.org/debian/dists/bullseye/main/binary-armel/...
http://mirrors.kernel.org/debian/dists/bullseye/contrib/binary-armel/...
```

Para configurar APT para utilizar una réplica específica, añada una línea como la siguiente (de nuevo, se presupone que está utilizando main y contrib):

```
deb http://mirrors.kernel.org/debian bullseye main contrib
```

Fíjese que "dists" se añade de forma implícita, y los parámetros tras el nombre de la versión se usan para expandir la ruta a varios directorios.

De nuevo, una vez añada las nuevas fuentes, deshabilite las entradas de archivo que tuviera previamente.

4.3.2. Añadir las réplicas locales para APT

En lugar de utilizar réplicas de paquetes remotos, puede que desee modificar el archivo de fuentes de APT para usar una réplica existente en su disco local (posiblemente montada mediante NFS).

Por ejemplo, su réplica de paquetes puede encontrarse en /var/local/debian/, y tener directorios como estos:

```
/var/local/debian/dists/bullseye/main/binary-armel/...
/var/local/debian/dists/bullseye/contrib/binary-armel/...
```

Para usar esta ubicación con apt debe añadir esta línea a su archivo sources.list:

```
deb file:/var/local/debian bullseye main contrib
```

Fíjese que "dists" se añade de forma implícita, y los parámetros tras el nombre de la versión se usan para expandir la ruta a varios directorios.

Tras añadir sus nuevas fuentes, desactive las líneas "deb" que había en los archivos de lista de fuentes de APT, colocando el símbolo de sostenido (#) delante de ellas.

4.3.3. Añadir fuentes para APT de medios ópticos

Si quiere utilizar *solamente* DVDs (o CDs, o discos Blu-ray), comente todas las líneas en los archivos de lista fuentes de APT colocando delante de ellas un símbolo de sostenido (#).

Asegúrese de que existe una línea en /etc/fstab que permita montar la unidad lectora de CD-ROMs en el punto de montaje /media/cdrom. Por ejemplo, si su lector de CD-ROM se encuentra en /dev/sr0, el archivo de configuración /etc/fstab debería incluir una línea similar a la siguiente:

```
/dev/sr0 /media/cdrom auto noauto,ro 0 0
```

Fíjese que *no debe haber espacios* entre las palabras noauto,ro en el cuarto campo.

Para verificar que esto funciona, inserte un CD e intente ejecutar

```
# mount /media/cdrom   # esto montará el CD en el punto de montaje
# ls -alF /media/cdrom # esto debería mostrar el directorio raíz del CD
# umount /media/cdrom  # esto desmontará el CD
```

Después, ejecute:

```
# apt-cdrom add
```

para añadir los datos a la base de datos de APT. Repita esta operación para cada CD-ROM de binarios de Debian que tenga.

4.4. Actualizar los paquetes

El método recomendado para actualizar de las versiones anteriores de Debian es utilizar la herramienta de gestión de paquetes **apt**.

NOTA

El programa **apt** está preparado para un uso interactivo, y no debería utilizarse en guiones. En guiones deberiá utilizar el programa **apt-get**, puesto que este último tiene una salida estable que está mucho más preparada para ser procesada.

No olvide montar todas las particiones que necesite (en particular la raíz y `/usr`) en modo lectura y escritura, con una orden como:

```
# mount -o remount,rw /punto_de_montaje
```

A continuación asegúrese de que las entradas con las fuentes de APT (en el archivo `/etc/apt/sources.list` y los archivos bajo `/etc/apt/sources.list.d/`) hacen referencia a la distribución "`bullseye`" o a estable ("`stable`"). No debería haber ninguna entrada que haga referencia a "`buster`".

NOTA

Las líneas de fuentes de un CD-ROM pueden hacen referencia a inestable ("`unstable`"), aunque esto le parezca confuso *no* debería cambiarlo.

4.4.1. Grabar la sesión

Se recomienda encarecidamente que utilice el programa **/usr/bin/script** para guardar una transcripción de la sesión de actualización. Así, si ocurre algún problema, tendrá un registro de lo que ha sucedido y, si fuera necesario, podrá proporcionar la información detallada cuando envíe un informe de fallo. Para iniciar la transcripción, teclee:

```
# script -t 2>~/actualiza-a-bullseye_paso_.time -a ~/actualiza-a-bullseye_paso_. ↩
    script
```

o similar. Si tiene que volver a ejecutar la transcripción (por ejemplo, si ha reiniciado el sistema) debería utilizar distintos valores de *`paso`* para indicar el paso de la actualización que se está transcribiendo. No ponga el archivo de transcripción en un directorio temporal como `/tmp` o `/var/tmp` (los archivos que hay en esos directorios se pueden borrar durante la actualización o durante el reinicio del sistema).

La transcripción también le permitirá revisar la información que se haya salido fuera de la pantalla. Simplemente acceda al terminal VT2 (utilizando Alt + F2) y, después de acceder al sistema, utilice `less -R ~root/actualiza-a-bullseye.script` para leer el archivo.

Después de completar la actualización puede terminar con la transcripción de **script** escribiendo `exit` en el indicador de línea de órdenes.

apt también registra los cambios de estado de los paquetes en `/var/log/apt/history.log` y en la salida de terminal en `/var/log/apt/term.log`. **dpkg** realizará, adicionalmente, un registro de todos los cambios de estado de los paquetes en `/var/log/dpkg.log`. Si utiliza **aptitude**, también dispondrá de un registro de los cambios de estado en `/var/log/aptitude`.

Si ha utilizado la opción *-t* para **script** puede utilizar el programa **scriptreplay** para reproducir la sesión completa:

```
# scripreplay ~/actualiza-a-bullseyepaso.time ~/actualiza-a-bullseyepaso.script
```

4.4.2. Actualizar las listas de paquetes

En primer lugar, tiene que descargar la lista con los paquetes disponibles para la nueva versión. Logrará esto si ejecuta:

```
# apt update
```

NOTA

Los usuarios de apt-secure pueden tener ciertos problemas cuando utilicen **aptitude** o **apt-get**. Para apt-get, puede utilizar la orden **apt-get update --allow-releaseinfo-change**.

4.4.3. Asegúrese de que tiene suficiente espacio libre para actualizar

Antes de actualizar su sistema tiene que asegurarse de que tendrá suficiente espacio libre en su disco duro para poder seguir las instrucciones de una actualización completa del sistema que se describen en Sección 4.4.5. En primer lugar, cualquier paquete que sea necesario para la instalación se descargará y se almacenará en `/var/cache/apt/archives` (y en el subdirectorio `partial/`, mientras se está descargando), por lo que necesitará suficiente espacio libre en la partición donde se encuentre `/var/` para poder descargar temporalmente los paquetes que se instalarán en su sistema. Después de la descarga, probablemente necesitará más espacio en las otras particiones de sistemas de ficheros para poder instalar tanto las actualizaciones de los paquetes (que podrían contener archivos binarios más grandes o más datos) como los nuevos paquetes que se necesiten en la actualización. Si su sistema no tiene suficiente espacio podría terminar con una actualización incompleta de la cual es difícil recuperarse.

La orden **apt** le puede mostrar información detallada del espacio libre necesario para la instalación. Puede consultar esa estimación, antes de proceder con la actualización, si ejecuta:

```
# apt -o APT::Get::Trivial-Only=true full-upgrade
[...]
XXX actualizados, XXX se instalará, XXX para eliminar y XXX no actualizados.
Se necesita descargar xx.xxMB de archivos.
Se utilizarán AAAMB de espacio de disco adicional después de esta operación.
```

NOTA

Puede que la ejecución de esta orden al principio del proceso de actualización genere un error, por las razones descritas en las siguientes secciones. En ese caso tiene que esperar para ejecutar esta orden hasta haber realizado una actualización mínima del sistema tal y como se describe en Sección 4.4.4 antes de ejecutar esta orden para poder estimar el espacio de disco necesario.

Si no tiene espacio suficiente para la actualización, **apt** le avisará con un mensaje como este:

```
E: No tiene suficiente espacio libre en /var/cache/apt/archives/.
```

Si no tiene espacio suficiente para la actualización, asegúrese de hacer sitio antes de proceder. Puede hacer lo siguiente:

- Elimine aquellos paquetes que se han descargado previamente para su instalación (en `/var/cache/apt/archive`). Puede utilizar la orden **apt clean** para borrar todos los archivos de paquetes previamente descargados.
- Eliminar paquetes olvidados. Si ha utilizado **aptitude** o **apt** para instalar manualmente paquetes de buster, la herramienta hará un seguimiento de los paquetes que haya instalado y podrá marcar como redundantes aquellos paquetes que se obtuvieron solo para cumplir las dependencias pero que ya no se necesitan porque el paquete que los necesitaba se ha eliminado. No se marcarán como obsoletos aquellos paquetes que haya instalado manualmente. Pero si lo hará para aquellos paquetes que se instalaron automáticamente para cumplir dependencias. Para eliminar automáticamente los paquetes instalados que no se necesitan puede ejecutar lo siguiente:

  ```
  # apt-get autoremove
  ```

  También puede utilizar para encontrar paquetes redundantes **deborphan**, **debfoster** o **cruft**. No elimine a ciegas los paquetes que le indiquen estas herramientas, especialmente si utiliza opciones agresivas, distintas a las definidas por omisión, que pueden dar lugar a muchos falsos positivos. Se le recomienda encarecidamente que revise los paquetes que éstas le sugieren eliminar (esto es: sus contenidos, su tamaño y descripción) antes de eliminarlos
- Elimine paquetes que consumen mucho espacio y que no necesita actualmente (siempre puede instalarlos después de la actualización). Puede utilizar la orden **popcon-largest-unused** para listar los paquetes que no utiliza que consumen más espacio si tiene instalado `popularity-contest`. Puede encontrar los paquetes que consumen más espacio con **dpigs** (disponible en el paquete `debian-goodies`) o con **wajig** (ejecutando `wajig size`). También puede encontrarlos con `aptitude`. Ejecute **aptitude** en el modo de terminal completo, seleccione Vistas y Nueva vista de paquetes plana, pulse la tecla **l** e introduzca `~i`, a continuación pulse la tecla **S** e introduzca `~installsize`. Una vez hecho esto, dispondrá de una lista de paquetes sobre la que puede trabajar.
- Puede eliminar las traducciones y los archivos de localización del sistema si no los necesita. Para ello puede instalar el paquete `localepurge`, configurándolo para que solo se mantengan en el sistema algunas localizaciones específicas. Esto reducirá el espacio de disco consumido en `/usr/share/locale`.
- Mueva de forma temporal a otro sistema o elimínelos de forma permanente, los registros del sistema que residen en `/var/log/`.
- Utilice una ubicación temporal para `/var/cache/apt/archives`: puede utilizar una caché temporal en otro sistema de archivos (USB, dispositivo de almacenamiento, espacio en disco duro temporal, sistema de ficheros en uso, etc.).

NOTA

No utilice un sistema montado a través de NFS dado que la conexión de red podría interrumpirse durante la actualización.

Por ejemplo, si tiene una unidad USB montada en `/media/usbkey`:

1. elimine los paquetes que se han descargado previamente para la instalación

```
# apt clean
```

2. copie los contenidos de `/var/cache/apt/archives` a la unidad USB:

```
# cp -ax /var/cache/apt/archives /media/usbkey/
```

3. monte el directorio de caché temporal sobre el actual:

```
# mount --bind /media/usbkey/archives /var/cache/apt/archives
```

4. después de la actualización, restaure el directorio original `/var/cache/apt/archives`

```
# umount /var/cache/apt/archives
```

5. elimine el directorio `/media/usbkey/archives`.

Puede crear una directorio de caché temporal en cualquier sistema de archivos montado en su sistema.

- Realice un actualización mínima del sistema (consulte Sección 4.4.4) o una actualización parcial seguida de una actualización completa del sistema. Esto le permitirá actualizar el sistema parcialmente, lo que le permitirá limpiar la caché de paquetes antes de la actualización completa.

Tenga en cuenta que para poder eliminar los paquetes con seguridad debería cambiar su `sources.list` a buster como se describe en Sección A.2.

4.4.4. Actualización mínima del sistema

IMPORTANTE

If you are upgrading remotely, be aware of Sección 5.1.22.

En algunos casos, la realización directamente de una actualización completa (como se describe más abajo) podría tener como consecuencia la eliminación de un buen número de paquetes que quiere conservar. Le recomendamos por tanto un proceso de actualización en dos pasos. En primer lugar, una actualización mínima para resolver estos conflictos, seguido de una actualización completa como se describe en Sección 4.4.5.

Para hacer esto, ejecute primero lo siguiente:

```
# apt upgrade --without-new-pkgs
```

Esto tiene como consecuencia que se actualicen los paquetes que se puedan actualizar en el sistema sin que sea necesario eliminar ni instalar ningún otro paquete.

La actualización mínima del sistema también puede ser útil cuando hay poco espacio libre disponible en el sistema y no puede ejecutarse la actualización completa debido a problemas de espacio.

Si está instalado el paquete `apt-listchanges`, mostrará (en su configuración por omisión) información importante sobre los paquetes actualizados en un paginador después de descargar los paquetes. Pulse **q** después de leer esta información para salir del paginador y continuar con la actualización.

4.4.5. Actualizar el sistema

Una vez haya realizado los pasos anteriores, estará en condiciones de seguir con la parte principal de la actualización. Ejecute:

```
# apt full-upgrade
```

Se realizará una actualización completa del sistema, esto es, se instalarán las versiones más recientes de los paquetes y se resolverán todos los posibles cambios de dependencias entre los paquetes de diferentes versiones. Si fuera necesario, se instalarán nuevos paquetes (normalmente, nuevas versiones de las bibliotecas o paquetes que han cambiado de nombre), y se eliminarán los paquetes obsoletos conflictivos.

Cuando esté actualizando desde un conjunto de CDs/DVDs/BDs, probablemente se le pedirá que inserte algunos discos específicos en distintos momentos durante la actualización. Puede que tenga que insertar el mismo disco varias veces; esto se debe a que algunos paquetes interrelacionados pueden estar dispersos en distintos discos.

Las versiones nuevas de los paquetes ya instalados que no se puedan actualizar sin cambiar el estado de la instalación de otro paquete se dejarán en su versión actual (en cuyo caso se mostrarán como «held back», es decir, «retenidos»). Se puede resolver esta incidencia usando **aptitude** para elegir esos paquetes para que se instalen, o intentando ejecutar `apt install` *`paquete`*.

4.5. Posibles problemas durante o después de la actualización

Las siguientes secciones describen problemas conocidos que pueden aparecer durante la actualización a bullseye.

4.5.1. Dist-upgrade falla con «No se pudo realizar la configuración inmediata»

En algunos casos el paso **apt full-upgrade** puede fallar después de descargar los paquetes con el siguiente error:

```
E: No se pudo realizar la configuración inmediata de «paquete». Consulte la ↩
    página de manual con «man 5 apt.conf» bajo «APT::Immediate-Configure» para ↩
    más información.
```

Si esto sucede, debería ejecutar la orden **apt full-upgrade -o APT::Immediate-Configure=0**, que permitirá continuar con la actualización.

Otra posible alternativa para evitar este problema es añadir temporalmente fuentes tanto de buster como de bullseye en los archivos de las fuentes APT y ejecutar **apt update**.

4.5.2. Eliminaciones esperadas

El proceso de actualización a bullseye puede solicitar la eliminación de paquetes en el sistema. La lista exacta de paquetes dependerá del conjunto de paquetes que tenga instalado. Estas notas de publicación proporcionan recomendaciones generales sobre estas eliminaciones pero, si tiene dudas, se recomienda que revise los paquetes que se van a eliminar propuestos por cada método antes de continuar. Encontrará más información de los paquetes obsoletos en bullseye en Sección 4.8.

4.5.3. Bucles en Conflictos o Pre-Dependencias

Algunas veces es necesario activar la opción `APT::Force-LoopBreak` en APT para permitir el borrado temporal de un paquete esencial debido a un bucle de Conflictos y Dependencias previas. **apt** le alertará de esta situación y abortará la actualización. Puede resolver esto especificando la opción `-o APT::Force-LoopBreak=1` en la línea de órdenes de **apt-get**.

Es posible que la estructura de dependencias del sistema esté tan dañada que precise de intervención manual. Normalmente, esto implica usar **apt** o

```
# dpkg --remove nombre_de_paquete
```

para eliminar algunos de los paquete problemáticos, o

```
# apt -f install
# dpkg --configure --pending
```

En casos extremos, puede que necesite forzar la reinstalación con una orden como:

```
# dpkg --install /ruta/al/nombre_de_paquete.deb
```

4.5.4. Conflictos de archivo

No deberían producirse conflictos entre archivos si actualiza de un sistema buster “puro”, pero sí pueden producirse si ha instalado versiones nuevas no oficiales («backports», N. del T.). Si se produce un conflicto entre archivos se mostrará con un error similar al siguiente:

```
Desempaquetando <paquete-foo> (de <paquete-foo-fichero>) ...
dpkg: error al procesar <paquete-foo> (--install):
 intentando sobreescribir '<algún-nombre-fichero>',
 que está también en el paquete <paquete-bar>
dpkg-deb: subprocess paste killed by signal (Broken pipe)
 Se encontraron errores al procesar:
 <paquete-foo>
```

Puede intentar resolver los conflictos entre archivos forzando a que se elimine el paquete mencionado en la *última* línea del mensaje de error:

```
# dpkg -r --force-depends nombre_de_paquete
```

Debería poder continuar la instalación donde la dejó tras corregir el problema repitiendo las órdenes de `apt` descritas previamente.

4.5.5. Cambios de configuración

Se le harán preguntas sobre la configuración o reconfiguración de diversos paquetes durante la actualización. Cuando se le pregunte si debería reemplazarse algún archivo en el directorio `/etc/init.d`, o el archivo `/etc/manpath.config` con la versión que propone el mantenedor del paquete, normalmente deberá responder “sí” para asegurar la consistencia del sistema. Siempre puede volver más tarde a las versiones antiguas, ya que quedan guardadas con la extensión `.dpkg-old`.

Si no está seguro de lo que debe hacer, anote el nombre del paquete o archivo, y revise la situación más adelante. Recuerde que podrá buscar en el archivo de transcripción de la instalación y revisar la información que apareció en pantalla durante la actualización.

4.5.6. Cambio de la sesión en consola

Si está Vd. ejecutando el proceso de actualización utilizando la consola local del sistema es posible que en algunos momentos durante la actualización se cambie la consola a una vista distinta y deje de ver el proceso de actualización. Esto puede suceder, por ejemplo, en sistemas con inerfaz gráfica cuando se reinicia el gestor de escritorios.

Para recuperar la consola donde se estaba realizando la actualización tendrá que utilizar la combinación de teclas Ctrl + Alt + F1 (si está en la pantalla de arranque gráfico) o Alt + F1 (si está en la consola de modo texto) para volver al terminal virtual 1. Reemplace F1 por la tecla de función que tenga el mismo número que el terminal virtual donde se estaba realizando la actualización. También puede utilizar la combinación Alt + Flecha Izquierda o Alt + Flecha Derecha para conmutar entre los distintos terminales de modo texto.

4.6. Actualización de su núcleo y paquetes relacionados

Esta sección explica cómo actualizar su núcleo e identifica los posibles problemas que pueden darse con relación a esta actualización. Puede o bien instalar uno de los paquetes `linux-image-*` que ofrece Debian o compilar un núcleo personalizado desde el código fuente del mismo.

Tenga en cuenta que gran parte de la información de esta sección se basa en la suposición de que está utilizando uno de los núcleos modulares de Debian, conjuntamente con `initramfs-tools` y `udev`. Parte de la información aquí presentada puede no ser relevante para usted si utiliza un núcleo a medida que no necesita un initrd o si utiliza un generador de initrd distinto.

4.6.1. Instalación de un metapaquete del núcleo

Cuando realice «full-upgrade» desde buster a bullseye, le recomendamos encarecidamente que instale uno de los nuevos metapaquetes «linux-image-*» si aún no lo ha hecho. Estos metapaquetes instalarán de forma automática una nueva versión del núcleo durante una actualización. Puede verificar si tiene uno ya instalado con la siguiente orden:

```
# dpkg -l "linux-image*" | grep ^ii | grep -i meta
```

Si no observa ningún mensaje, entonces necesitará instalar un nuevo paquete «linux-image» a mano o instalar un metapaquete «linux-image». Para ver una lista de los metapaquetes «linux-image» disponibles, ejecute:

```
# apt-cache search linux-image- | grep -i meta | grep -v transition
```

Si no está seguro de qué paquete instalar, ejecute la orden `uname -r` y busque un paquete con un nombre similar. Por ejemplo, si ve "`4.9.0-8-amd64`", le recomendamos que instale `linux-image-amd64`. También puede utilizar **apt-cache** para ver una descripción más larga de cada uno de los paquetes para así ayudarle a realizar una mejor elección de entre los que hay disponibles. Por ejemplo:

```
# apt show linux-image-amd64
```

Luego debería usar `apt install` para instalarlo. Debería reiniciar en cuanto le sea posible una vez que haya instalado el núcleo nuevo para empezar a beneficiarse de las características que proporciona la nueva versión del núcleo. Sin embargo, debe leer primero Sección 5.1.24 antes de hacer el primer reinicio tras una actualización.

Para los más aventureros, hay una forma fácil para compilar su propio núcleo a medida en Debian. Instale las fuentes del núcleo, que se incluyen en el paquete `linux-source`. Puede utilizar el objetivo `deb-pkg` disponible en el fichero Makefile de los paquetes fuentes utilizados para construir un paquete binario. Puede encontrar más información en el Debian Linux Kernel Handbook (`https://kernel-team.pages.debian.net/kernel-handbook/`), que también está disponible en el paquete `debian-kernel-handbook`."

Siempre que sea posible, es mejor para usted si actualiza el paquete del núcleo de forma independiente a la actualización principal con `full-ugprade`, para así reducir las posibilidades de tener durante un cierto periodo de tiempo un sistema que no se puede iniciar. Tenga en cuenta que solo debería hacer esto después de haber realizado el proceso de actualización mínima del sistema que se describe en Sección 4.4.4.

4.7. Prepararse para la siguiente distribución

Una vez hecha la actualización hay ciertas cosas que puede hacer para prepararse para la siguiente versión de la distribución.

- Elimine los paquetes redundantes y obsoletos tal y como se describe en Sección 4.8. Debería revisar qué archivos de configuración utilizan y considerar como opción purgarlos para eliminar sus archivos de configuración. También puede consultar la sección Sección 4.7.1.

4.7.1. Purgando los paquetes eliminados

En general es recomendable purgar los paquetes eliminados. Esto es particularmente necesario si se han eliminado en una actualización anterior (p.ej. por la actualización a buster) o eran parte de paquetes de terceros. Se han dado muchos casos en los que los programas de init.d antiguos han causado problemas.

> ATENCIÓN
>
> 
>
> En general, al purgar un paquete también se purgarán sus ficheros de registro. Por lo que puede ser recomendable hacer una copia de seguridad de éstos antes de hacerlo.

La siguiente orden mostrará una lista de todos los paquetes eliminados que puedan haber dejado ficheros de configuración en el sistema (si los hay):

```
# dpkg -l | awk '/^rc/ { print $2 }'
```

Los paquetes puede eliminarse utilizando **apt purge**. Si lo que quiere es eliminarlos todos de un solo golpe, puede utilizar la siguiente orden:

```
# apt purge $(dpkg -l | awk '/^rc/ { print $2 }')
```

Si utiliza `aptitude`, también puede utilizar las siguientes órdenes de forma alternativa a las listadas antes:

```
# aptitude search '~c'
# aptitude purge '~c'
```

4.8. Paquetes obsoletos

La versión bullseye, aunque introduce muchos paquetes nuevos, también retira o deja de distribuir algunos paquetes que estaban disponibles en buster. No existe un mecanismo de actualización para estos paquetes obsoletos. Aunque nada le impide que siga usando paquetes obsoletos si así lo desea, el proyecto Debian deja de dar soporte de seguridad para éstos un año después de la publicación de bullseye[5] y no se ofrecerá otro tipo de soporte durante este tiempo. Lo recomendable es reemplazar dichos paquetes con las alternativas disponibles, si es que existen.

Hay muchas razones por las que un paquete puede haberse eliminado de la distribución, a saber: no hay mantenimiento por parte de los desarrolladores originales, no hay ningún desarrollador en Debian que esté interesado en mantener los paquetes, la funcionalidad que ofrecen la ofrece ahora otros programas (o una nueva versión), o ya no se consideran aptos para distribuirse en bullseye debido a los errores que presentan. En este último caso los paquetes puede que sigan estando presentes en la distribución “inestable”.

Algunos interfaces de gestión de paquetes ofrecen una forma fácil para encontrar los paquetes instalados que ya no están disponibles en ningún repositorio conocido. El interfaz de texto de **aptitude** los lista dentro de la categoría “Paquetes obsoletos y creados locamente”, y pueden listarse y purgarse desde la línea de órdenes con:

```
# aptitude search '~o'
# aptitude purge '~o'
```

[5] O hasta que se publique una nueva versión en ese tiempo. Habitualmente solo se da soporte a dos versiones estables en un momento determinado.

A menudo podrá encontrar más información de por qué un paquete fue eliminado en el Sistema de seguimiento de fallos de Debian (`https://bugs.debian.org/`). Debería consultar tanto los informes de fallos del propio paquete como los informes de fallos archivados del pseudo-paquete ftp.debian.org (`https://bugs.debian.org/cgi-bin/pkgreport.cgi?pkg=ftp.debian.org&archive=yes`).

Puede consultar una lista de los paquetes obsoletos de Bullseye en Sección 5.3.1.

4.8.1. Paquetes «dummy» de transición

Algunos de los paquetes de buster pueden haber sido reemplazados por paquetes «dummy» de transición, que son paquetes vacíos diseñados simplemente para facilitar la actualización. Por ejemplo, si una aplicación que antes estaba en un paquete se ha dividido en varios, puede proporcionarse un paquete de transición con el mismo nombre que el paquete antiguo y con las dependencias adeucadas para que se instalen los nuevos paquetes. Después de haber realizado ésto el paquete «dummy» es redundante y puede borrarse sin consecuencias.

La mayoría (pero no todas) de las descripciones de los paquetes «dummy» indican su propósito. Sin embargo, las descripciones de estos paquetes no son uniformes, en particular algunos paquetes «dummy» no están pensados para ser eliminados después de una actualización sino que se utilizan para poder seguir a lo largo del tiempo la versión más reciente de un programa. Puede que encuentre útil utilizar **deborphan** con las opciones `--guess-*` (p.ej. `--guess-dummy`) para detectar los que están instalados en su sistema.

Capítulo 5

Problemas que debe tener en cuenta para bullseye

Algunas veces los cambios tienen efectos colaterales que no podemos evitar, o aparecen fallos en otro lugar. A continuación se documentan los problemas que conocemos. Puede leer también la fe de erratas, la documentación de los paquetes relevantes, los informes de fallos y otra información mencionada en Sección 6.1.

5.1. Actualizar elementos específicos para bullseye

Esta sección cubre los elementos relacionados con la actualización de buster a bullseye

5.1.1. El sistema de ficheros XFS no da soporte a la opción barrier/nobarrier

Se ha eliminado el soporte para las opciones de montaje `barrier` y `nobarrier` del sistema de ficheros XFS. Es recomendable revisar si se utilizan estas opciones en la configuración de `/etc/fstab` y eliminarlas si es el caso. Las particiones que utilicen estos parámetros no podrán montarse.

5.1.2. Cambio de la organización del archivo de seguridad

For bullseye, the security suite is now named `bullseye-security` instead of *codename*`/updates` and users should adapt their APT source-list files accordingly when upgrading.

La línea de seguridad en su configuración de APT puede ser similar a la siguiente:

```
deb https://deb.debian.org/debian-security bullseye-security main contrib
```

If your APT configuration also involves pinning or `APT::Default-Release`, it is likely to require adjustments as the codename of the security archive no longer matches that of the regular archive. An example of a working `APT::Default-Release` line for bullseye looks like:

```
APT::Default-Release "/^bullseye(|-security|-updates)$/";
```

which takes advantage of APT's support for regular expressions (inside `/`).

5.1.3. Los hash de contraseña utilizan yescrypt por omisión

El hash por omisión de contraseñas para cuentas del sistema locales se ha modificado (`https://tracker.debian.org/news/1226655/accepted-pam-140-3-source-into-unstable/`) de SHA-512 a yescrypt (`https://www.openwall.com/yescrypt/`) (consulte crypt(5) (`https://manpages.debian.org//bullseye/libcrypt-dev/crypt.5.html`)). Se espera que este cambio mejore la seguridad contra ataques de fuerza bruta de diccionario, tanto desde el punto de vista de la complejidad del espacio de claves y del tiempo necesario para llevar a cabo este tipo de ataques.

Para aprovecharse de esta mejora de seguridad, ha de modificar las contraseñas locales. Por ejemplo, puede utilizar la orden **passwd**.

Las contraseñas antiguas seguirán utilizando el hash de contraseña que se utilizó cuando éstas se crearon.

No hay soporte de «yescrypt» en Debian 10 (buster). Como consecuencia de esto, no pueden copiarse los archivos de contraseñas shadow en (`/etc/shadow`) de un sistema bullseye a un sistema buster. Si se copian estos archivos, las contraseñas que se han modificado en el sistema bullseye no funcionarán en el sistema buster system. De forma similar, los hashes de contraseñas no pueden cortar y copiarse de un sistema bullseye a un sistema buster.

Si necesita compatibilidad para los hashes de contraseña entre bullseye y buster, modifique `/etc/pam.d/common-password`. Debe buscar la línea que sea parecida a:

```
password [success=1 default=ignore] pam_unix.so obscure yescrypt
```

y reemplazar `yescrypt` con `sha512`.

5.1.4. El soporte de NSS NIS y NIS+ requiere nuevos paquetes

El soporte de NSS NIS y NIS+ se ha movido a paquetes separados nombrados `libnss-nis` y `libnss-nisplus`. Desgraciadamente, `glibc` no puede depender de esos paquetes, por lo que son sólo recomendados.

Por tanto es recomendable en aquellos sistemas que utilicen NIS o NIS+ que esos paquetes están correctamente instalados antes de la actualización.

5.1.5. Gestión de fragmentos de configuración en unbound

El gestor de DNS `unbound` ha modificado la forma en la que gestiona archivos de fragmentos de configuración. Si depende de la directiva `include:` para unir varios fragmentos en un archivo de configuración válido debería leer el archivo NEWS (`https://sources.debian.org/src/unbound/bullseye/debian/NEWS/`).

5.1.6. Parámetros obsoletos de rsync

The `rsync` parameters `--copy-devices` and `--noatime` have been renamed to `--write-devices` and `--open-noatime`. The old forms are no longer supported; if you are using them you should see the NEWS file (`https://sources.debian.org/src/rsync/bullseye/debian/rsync.NEWS/`). Transfer processes between systems running different Debian releases may require the buster side to be upgraded to a version of `rsync` from the backports (`https://backports.debian.org/`) repository.

5.1.7. Gestión de complementos de Vim

Los complementos para `vim` que anteriormente se proporcionaban en `vim-scripts` se gestionan ahora de forma nativa a través de la funcionalidad nativa de Vim de “paquetes” en lugar de a través de `vim-addon-manager`. Los usuarios de Vim deberían prepararse antes de la actualización siguiendo las instrucciones descritas en el archivo NEWS (`https://sources.debian.org/src/vim-scripts/bullseye/debian/NEWS/`).

5.1.8. OpenStack y cgroups v1

OpenStack Victoria (publicado in bullseye) requiere cgroup v1 para QoS de los dispositivos de bloque. Dado que bullseye también cambia y utiliza cgroupv2 por omisión (consulte Sección 2.2.4), el arbol sysfs en `/sys/fs/cgroup` no incluye funcionalidades de cgroup v1 como `/sys/fs/cgroup/blkio`. Como consecuencia de ésto la ejecución de **cgcreate -g blkio:foo** fallará. En aquellos nodos OpenStack que estén ejecutando `nova-compute` o `cinder-volume` es muy recomendable añadir los parámetros `systemd.unified_cgroup_hierarchy=false` y `systemd.legacy_systemd_cgroup_controller=false` a la línea de órdenes del núcleo. Esto hará que se deje de utilizar el valor por omisión y se restaure la jerarquía antigua de cgroup.

5.1.9. Archivos de política de OpenStack API

Siguiendo las recomendaciones de los desarrolladores originales, la versión Victoria de OpenStack que se publica en bullseye cambia la API de OpenStack para utilizar el nuevo formato YAML. Como consecuencia de ésto, la mayor parte de los servicios de OpenStack (como Nova, Glance, y Keystone) parecen rotos con todos los archivos de políticas de API escritos de forma explícita en archivos `policy.json`. Los paquetes ahora incluyen un directorio `/etc/PROJECT/policy.d` que contiene un archivo `00_default_policy.yaml`. Este archivo tiene todas las políticas comentadas por omisión.

Para impedir que el antiguo fichero `policy.json` esté activo, los paquetes de OpenStack en Debian renombran este archivo a `disabled.policy.json.old`. En aquellos casos en los que no se podía hacer nada mejor antes de la publicación el archivo `policy.json` simplemente se borra. Antes de actualizar se recomienda encarecidamente hacer una copia de seguridad de los archivos `policy.json` en su despliegue.

Puede encontrar más detalles en la documentación original del producto (`https://governance.openstack.org/tc/goals/selected/wallaby/migrate-policy-format-from-json-to-yaml.html`).

5.1.10. Indisponibilidad de sendmail durante la actualización

A diferencia de las actualizaciones normales de `sendmail`, el servicio de sendmail se parará durante la actualización de buster a bullseye the sendmail. Esto causará que el servicio no esté disponible durante más tiempo del habitual. Puede leer algunos consejos genéricos para reducir los tiempos de indisponibilidad en Sección 4.1.3 .

5.1.11. FUSE 3

Algunos paquetes se han movido a FUSE 3, esto incluye algunos paquetes como `gvfs-fuse`, `kio-fuse`, y `sshfs`. Esto provocará que durante la actualización se instale `fuse3` y se elimine `fuse` .

En algunas circunstancias excepciones pueden retenerse los paquetes que dependen de `fuse3` durante la actualización. Esto puede suceder, por ejemplo, si realiza la actualización ejecutando sólamente **apt-get dist-upgrade** en lugar de los pasos recomendados de actualización en Capítulo 4. Se puede resolver la situación si ejecuta de nuevo los pasos que se indican en Sección 4.4.5 con la versión de bullseye de `apt` o si los actualiza manualmente.

5.1.12. GnuPG options file

Starting with version 2.2.27-1, per-user configuration of the `GnuPG` suite has completely moved to `~/.gnupg/gpg.conf`, and `~/.gnupg/options` is no longer in use. Please rename the file if necessary, or move its contents to the new location.

5.1.13. Linux enables user namespaces by default

From `Linux` 5.10, all users are allowed to create user namespaces by default. This will allow programs such as web browsers and container managers to create more restricted sandboxes for untrusted or less-trusted code, without the need to run as root or to use a setuid-root helper.

The previous Debian default was to restrict this feature to processes running as root, because it exposed more security issues in the kernel. However, as the implementation of this feature has matured, we are now confident that the risk of enabling it is outweighed by the security benefits it provides.

If you prefer to keep this feature restricted, set the sysctl:

```
user.max_user_namespaces = 0
```

Note that various desktop and container features will not work with this restriction in place, including web browsers, `WebKitGTK`, `Flatpak` and `GNOME` thumbnailing.

The Debian-specific sysctl `kernel.unprivileged_userns_clone=0` has a similar effect, but is deprecated.

5.1.14. Linux disables unprivileged calls to bpf() by default

From Linux 5.10, Debian disables unprivileged calls to bpf() by default. However, an admin can still change this setting later on, if needed, by writing 0 or 1 to the kernel.unprivileged_bpf_disabled sysctl.

If you prefer to keep unprivileged calls to bpf() enabled, set the sysctl:

```
kernel.unprivileged_bpf_disabled = 0
```

For background on the change as default in Debian see bug 990411 (https://bugs.debian.org/990411) for the change request.

5.1.15. redmine missing in bullseye

The package redmine is not provided in bullseye, as it was too late migrating over from the old version of rails which is at the end of upstream support (receiving fixes for severe security bugs only) to the version which is in bullseye. The Ruby Extras Maintainers are following upstream closely and will be releasing a version via backports (https://backports.debian.org/) as soon as it is released and they have working packages. If you can't wait for this to happen before upgrading, you can use a VM or container running buster to isolate this specific application.

5.1.16. Exim 4.94

Please consider the version of Exim in bullseye a *major* Exim upgrade. It introduces the concept of tainted data read from untrusted sources, like e.g. message sender or recipient. This tainted data (e.g. $local_part or $domain) cannot be used among other things as a file or directory name or command name.

This *will break* configurations which are not updated accordingly. Old Debian Exim configuration files also will not work unmodified; the new configuration needs to be installed with local modifications merged in.

Typical nonworking examples include:

- Delivery to /var/mail/$local_part. Use $local_part_data in combination with check_local_user.
- Using

  ```
  data = ${lookup{$local_part}lsearch{/some/path/$domain/aliases}}
  ```

  instead of

  ```
  data = ${lookup{$local_part}lsearch{/some/path/$domain_data/aliases}}
  ```

  for a virtual domain alias file.

The basic strategy for dealing with this change is to use the result of a lookup in further processing instead of the original (remote provided) value.

To ease upgrading there is a new main configuration option to temporarily downgrade taint errors to warnings, letting the old configuration work with the newer Exim. To make use of this feature add

```
.ifdef _OPT_MAIN_ALLOW_INSECURE_TAINTED_DATA
 allow_insecure_tainted_data = yes
.endif
```

to the Exim configuration (e.g. to /etc/exim4/exim4.conf.localmacros) *before* upgrading and check the logfile for taint warnings. This is a temporary workaround which is already marked for removal on introduction.

5.1.17. SCSI device probing is non-deterministic

Due to changes in the Linux kernel, the probing of SCSI devices is no longer deterministic. This could be an issue for installations that rely on the disk probing order. Two possible alternatives using links in `/dev/disk/by-path` or a `udev` rule are suggested in this mailing list post (`https://lore.kernel.org/lkml/59eedd28-25d4-7899-7c3c-89fe7fdd4b43@acm.org/`).

5.1.18. rdiff-backup require lockstep upgrade of server and client

The network protocol of versions 1 and 2 of `rdiff-backup` are incompatible. This means that you must be running the same version (either 1 or 2) of `rdiff-backup` locally and remotely. Since buster ships version 1.2.8 and bullseye ships version 2.0.5, upgrading only the local system or only the remote system from buster to bullseye will break `rdiff-backup` runs between the two.

Version 2.0.5 of `rdiff-backup` is available in the buster-backports archive, see backports (`https://backports.debian.org/`). This enables users to first upgrade only the `rdiff-backup` package on their buster systems, and then independently upgrade systems to bullseye at their convenience.

5.1.19. Intel CPU microcode issues

The `intel-microcode` package currently in bullseye and buster-security (see DSA-4934-1 (`https://www.debian.org/security/2021/dsa-4934`)) is known to contain two significant bugs. For some CoffeeLake CPUs this update may break network interfaces (`https://github.com/intel/Intel-Linux-Processor-Microcode-Data-Files/issues/56`) that use `firmware-iwlwifi`, and for some Skylake R0/D0 CPUs on systems using a very outdated firmware/BIOS, the system may hang on boot (`https://github.com/intel/Intel-Linux-Processor-Microcode-Data-Files/issues/31`).

If you held back the update from DSA-4934-1 due to either of these issues, or do not have the security archive enabled, be aware that upgrading to the `intel-microcode` package in bullseye may cause your system to hang on boot or break iwlwifi. In that case, you can recover by disabling microcode loading on boot; see the instructions in the DSA, which are also in the `intel-microcode` `README.Debian`.

5.1.20. Upgrades involving libgc1c2 need two runs

Packages that depend on `libgc1c2` in buster (e.g. `guile-2.2-libs`) may be held back during the first full upgrade run to bullseye. Doing a second upgrade normally solves the issue. The background of the issue can be found in bug #988963 (`https://bugs.debian.org/988963`).

5.1.21. fail2ban can't send e-mail using mail from bsd-mailx

The `fail2ban` package can be configured to send out e-mail notifications. It does that using **mail**, which is provided by multiple packages in Debian. A security update (needed on systems that use **mail** from `mailutils`) just before the release of bullseye broke this functionality for systems that have **mail** provided by `bsd-mailx`. Users of `fail2ban` in combination with `bsd-mailx` who wish `fail2ban` to send out e-mail should either switch to a different provider for **mail** or manually unapply the upstream commit (`https://github.com/fail2ban/fail2ban/commit/410a6ce5c80dd981c22752da034f2529b5e`) (which inserted the string "`-E 'set escape'`" in multiple places under `/etc/fail2ban/action.d/`).

5.1.22. No new SSH connections possible during upgrade

Although existing Secure Shell (SSH) connections should continue to work through the upgrade as usual, due to unfortunate circumstances the period when new SSH connections cannot be established is longer than usual. If the upgrade is being carried out over an SSH connection which might be interrupted, it's recommended to upgrade `openssh-server` before upgrading the full system.

5.1.23. Open vSwitch upgrade requires interfaces(5) change

The `openvswitch` upgrade may fail to recover bridges after boot. The workaround is:

```
sed -i s/^allow-ovs/auto/ /etc/network/interfaces
```

For more info, see bug #989720 (https://bugs.debian.org/989720).

5.1.24. Cosas a hacer después de la actualización y antes de reiniciar

Cuando haya terminado `apt full-upgrade` la actualización "formal" se habrá completado. No hay que hacer ninguna acción especial antes del siguiente reinicio del sistema tras la actualización a bullseye.

5.2. Elementos no limitados durante el proceso de actualización

5.2.1. Limitaciones en el soporte de seguridad

Hay algunos paquetes para los que Debian no puede comprometerse a proporcionar versiones actualizadas resolviendo problemas de seguridad. La información de estos paquetes se cubre en las siguientes subsecciones.

NOTA

El paquete `debian-security-support` ayuda a supervisar el estado de soporte de seguridad de los paquetes instalados en el sistema.

5.2.1.1. Estado de seguridad en los navegadores web y sus motores de render

Debian 11 includes several browser engines which are affected by a steady stream of security vulnerabilities. The high rate of vulnerabilities and partial lack of upstream support in the form of long term branches make it very difficult to support these browsers and engines with backported security fixes. Additionally, library interdependencies make it extremely difficult to update to newer upstream releases. Therefore, browsers built upon e.g. the webkit and khtml engines[1] are included in bullseye, but not covered by security support. These browsers should not be used against untrusted websites. The webkit2gtk and wpewebkit engines *are* covered by security support.

Para la navegación web general se recomienda utilizar Firefox o Chromium. Se mantendrá actualizadas recompilando las versiones ESR más recientes para estable. La misma estrategia se aplicará a Thunderbird.

5.2.1.2. OpenJDK 17

Debian bullseye incluye una versión temprana de `OpenJDK 17` (la siguiente versión `OpenJDK LTS` después de `OpenJDK 11`), para evitar el proceso tedioso de arranque entre versiones. El plan es que `OpenJDK 17` reciba una actualización en bullseye a la versión que se publique en octubre de 2021. A esto le seguirá la publicación de actualizaciones de seguridad según lo permitan los recursos disponibles. Los usuarios no deberían tener la expectativa de ver actualizaciones de seguridad para cada actualización cuatrimestral de parches de seguridad.

5.2.1.3. Go-based packages

The Debian infrastructure currently has problems with rebuilding packages of types that systematically use static linking. Before buster this wasn't a problem in practice, but with the growth of the Go ecosystem it means that Go-based packages will be covered by limited security support until the infrastructure is improved to deal with them maintainably.

[1] These engines are shipped in a number of different source packages and the concern applies to all packages shipping them. The concern also extends to web rendering engines not explicitly mentioned here, with the exception of webkit2gtk and the new wpewebkit.

If updates are warranted for Go development libraries, they can only come via regular point releases, which may be slow in arriving.

5.2.2. Acceso de la configuración de GNOME sin ratón

No hay una forma directa de cambiar la configuración en la aplicación de Configuración de GNOME ofrecida por `gnome-control-center` sin un dispositivo apuntador. Como alternativa, puede navegar de la barra lateral al contenido principal pulsando dos veces **Flecha derecha**. Para volver a la barra lateral, puede empezar a escribir con Ctrl + F, escriba algo y luego pulse **Esc** para cancelar la búsqueda. Ahora puede utilizar las teclas **Flecha arriba** y **Flecha abajo** para navegar a la barra lateral. No es posible seleccionar resultados con el teclado.

5.2.3. La opción de arranque `rescue` no se puede utilizar sin la contraseña de root

El arranque con la opción `rescue` requiere la contraseña de root desde la implementación de `sulogin` que se utiliza desde since buster. El modo rescate no puede utilizarse si no se ha configurado una contraseña. Sin embargo, aún es posible arrancar con el párametro del núcleo `init=/sbin/sulogin --force`

Puede configurar systemd para hacer el equivalente a esto cuando se arranca en modo de rescate (también conocido como modo de un solo usuario, consulte: systemd(1) (`https://manpages.debian.org//bullseye/systemd/systemd.1.html`)) ejecutando **sudo systemctl edit rescue.service** y crear un archivo diciendo simplemente:

```
[Service]
Environment=SYSTEMD_SULOGIN_FORCE=1
```

También puede ser útil hacer ésto (o en su lugar) en la unidad de servicio `emergency.service`. Esta unidad se ejecuta *automáticamente* cuando se producen ciertos errores (consulte systemd.special(7) (`https://manpages.debian.org//bullseye/systemd/systemd.special.7.html`)), o cuando se añade la opción `emergency` la línea de órdenes del núcleo (p.ej. si el sistema no puede recuperarse utilizando el modo de rescate).

Para conocer más del trasfondo de este cambio y leer una discusión sobre las implicaciones de seguridad puede consultar #802211 (`https://bugs.debian.org//802211`).

5.3. Obsolescencia y deprecación

5.3.1. Paquetes obsoletos notables

A continuación se muestra una lista de los paquetes conocidos y notables que ahora están obsoletos (consulte Sección 4.8 para obtener una descripción).

La lista de paquetes obsoletos incluye:

- Se ha eliminado el paquete `lilo` de bullseye. El sucesor como cargador de arranque de lilo `grub2`.
- El gestor de listas Mailman versión 3 es la única versión disponible de Mailman de esta publicación. Se ha dividido Mailman en distintos componentes: el componente core está disponible en el paquete `mailman3` y el conjunto completo puede obtenerse a través del metapaquete `mailman3-full`.

  La versión antigua de Mailman 2.1 ya no está disponible (este solía ser el paquete `mailman`). Esta versión depende de Python 2 que ya no está disponible en Debian.

  Puede consultar instrucciones para hacer la actualización en la documentación de migración del proyecto. (`https://docs.mailman3.org/en/latest/migration.html`)
- El núcleo Linux no provee soporte para `isdn4linux` (i4l). Como consecuencia de esto se han eliminado del archivo todos los paquetes relacionados que proporcionan herramientas para el espacio de usuario: `isdnutils`, `isdnactivecards`, `drdsl` y `ibod`.

- Ya no se proveen las librerias antiguas libappindicator. Como consecuencia de ésto ya no están disponibles los paquetes asociados `libappindicator1`, `libappindicator3-1` y `libappindicator-dev`. Es de esperar que esto cause problemas de dependencias para programas de terceros que siguen dependiendo de libappindicator para mostrar notificaciones en la barra del sistema o que necesitan soporte de indicaciones.

  Debian utiliza `libayatana-appindicator` para reemplazar a libappindicator. Puede consultar el transfondo técnico en este anuncio (`https://lists.debian.org/debian-devel/2018/03/msg00506.html`).

- Debian ya no provee `chef`. Si utiliza Chef para la gestión de configuraciones, posiblemente el mejor camino de actualización es utilizar los paquetes disponibles en Chef Inc (`https://www.chef.io/`).

  Puede consultar las razones de su eliminación en la solicitud de eliminación (`https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=963750`).

- Python 2 está fuera de su fin de vida y ya no recibe actualizaciones de seguridad. No hay soporte en aplicaciones que se ejecuten en este intérprete y los paquetes que dependían de éste se han migrado a Python 3 o se han eliminado. Sin embargo, Debian bullseye aún incluye la versión de Python 2.7, así como un pequeño conjunto de herramientas de construcción de Python 2 como `python-setuptools`. Estos paquetes están disponibles solamente porque se requiere para los procesos de construcción de algunos paquetes que aún no han migrado a Python 3.

- The `aufs-dkms` package is not part of bullseye. Most `aufs-dkms` users should be able to switch to `overlayfs`, which provides similar functionality with kernel support. However, it's possible to have a Debian installation on a filesystem that is not compatible with `overlayfs`, e.g. `xfs` without `d_type`. Users of `aufs-dkms` are advised to migrate away from `aufs-dkms` before upgrading to bullseye.

- The network connection manager `wicd` will no longer be available after the upgrade, so to avoid the danger of losing connectivity users are recommended to switch before the upgrade to an alternative such as `network-manager` or `connman`.

5.3.2. Componentes obsoletos de bullseye

Con la publicación de Debian 12 (nombre en clave bookworm) algunas funcionalidades estarán obsoletas. Los usuarios deben migrar a otras alternativas para evitar problemas al actualizar a Debian 12.

Esto incluye las siguientes funcionalidades:

- Ya no aplican las justificaciones históricas que llevaban a la necesidad de tener una organización del sistema de ficheros con directorios `/bin`, `/sbin`, y `/lib` separados de sus directorios equivalentes bajo `/usr`. Consulte el resumen de Freedesktop.org (`https://www.freedesktop.org/wiki/Software/systemd/TheCaseForTheUsrMerge`). Debian bullseye será la última publicación de Debian que proporcione soporte para una organización del sistema de ficheros en la que usr no está unido a los demás. Aquellos sistemas que tienen una organización antigua que se han actualizado sin reinstalar pueden utilizar el paquete `usrmerge` para hacer la conversión si fuera necesario.

- bullseye es la última publicación de Debian que incluye la orden **apt-key**. Las claves deberían gestionarse dejando los ficheros en el directorio `/etc/apt/trusted.gpg.d`, utilizando el formato binario tal y como se crea con **gpg --export** con la extensión `.gpg`, o en formato ASCII protegido con la extensión `.asc`.

  Se ha planeado un reemplazado para la orden **apt-key list** que permita investigar el anillo de claves manualmente, pero aún no se ha empezado a trabajar en éste.

- The `slapd` database backends slapd-bdb(5) (`https://manpages.debian.org//bullseye/slapd/slapd-bdb.5.html`), slapd-hdb(5) (`https://manpages.debian.org//bullseye/slapd/slapd-hdb.5.html`), and slapd-shell(5) (`https://manpages.debian.org//bullseye/slapd/slapd-shell.5.html`) are being retired and will not be included in Debian 12. LDAP

databases using the bdb or hdb backends should be migrated to the slapd-mdb(5) (https://manpages.debian.org//bullseye/slapd/slapd-mdb.5.html) backend.

Additionally, the slapd-perl(5) (https://manpages.debian.org//bullseye/slapd/slapd-perl.5.html) and slapd-sql(5) (https://manpages.debian.org//bullseye/slapd/slapd-sql.5.html) backends are deprecated and may be removed in a future release.

The OpenLDAP Project does not support retired or deprecated backends. Support for these backends in Debian 11 is on a best effort basis.

5.3.3. No-longer-supported hardware

For a number of armel-based devices that were supported in buster, it is no longer viable for Debian to build the required Linux kernel, due to hardware limitations. The unsupported devices are:

- QNAP Turbo Station (TS-xxx)
- HP Media Vault mv2120

Users of these platforms who wish to upgrade to bullseye nevertheless should keep the buster APT sources enabled. Before upgrading they should add an APT preferences file containing:

```
Package: linux-image-marvell
Pin: release n=buster
Pin-Priority: 900
```

The security support for this configuration will only last until buster's End Of Life.

5.4. Known severe bugs

Although Debian releases when it's ready, that unfortunately doesn't mean there are no known bugs. As part of the release process all the bugs of severity serious or higher are actively tracked by the Release Team, so an overview of those bugs (https://bugs.debian.org/cgi-bin/pkgreport.cgi?users=release.debian.org@packages.debian.org;tag=bullseye-can-defer) that were tagged to be ignored in the last part of releasing bullseye can be found in the Debian Bug Tracking System (https://bugs.debian.org/). The following bugs were affecting bullseye at the time of the release and worth mentioning in this document:

Bug number	Package (source or binary)	Description
922981 (https://bugs.debian.org/922981)	ca-certificates-java	ca-certificates-java: /etc/ca-certificates/update.d/jks-keystore doesn't update /etc/ssl/certs/java/cacerts
990026 (https://bugs.debian.org/990026)	cron	cron: Reduced charset in MAILTO causes breakage
991081 (https://bugs.debian.org/991081)	gir1.2-diodon-1.0	gir1.2-diodon-1.0 lacks dependencies
990318 (https://bugs.debian.org/990318)	python-pkg-resources	python-pkg-resources: please add Breaks against the unversioned python packages
991449 (https://bugs.debian.org/991449)	fail2ban	fix for CVE-2021-32749 breaks systems with mail from bsd-mailx
990708 (https://bugs.debian.org/990708)	mariadb-server-10.5,galera	mariadb-server-10.5: upgrade problems due to galera-3 -> galera-4 switch
980429 (https://bugs.debian.org/980429)	src:gcc-10	g++-10: spurious c++17 mode segmentation fault in append_to_statement_list_1 (tree-iterator.c:65)

Bug number	Package (source or binary)	Description
980609 (https://bugs.debian.org/980609)	src:gcc-10	missing i386-cpuinfo.h
984574 (https://bugs.debian.org/984574)	gcc-10-base	gcc-10-base: please add Breaks: gcc-8-base (<< 8.4)
984931 (https://bugs.debian.org/984931)	git-el	git-el,elpa-magit: fails to install: /usr/lib/emacsen-common/packages/install/git emacs failed at /usr/lib/emacsen-common/lib.pl line 19, <TSORT> line 7.
987264 (https://bugs.debian.org/987264)	git-el	git-el: fails to install with xemacs21
991082 (https://bugs.debian.org/991082)	gir1.2-gtd-1.0	gir1.2-gtd-1.0 has empty Depends
948739 (https://bugs.debian.org/948739)	gparted	gparted should not mask .mount units
984714 (https://bugs.debian.org/984714)	gparted	gparted should suggest exfatprogs and backport the commit that rejects exfat-utils
968368 (https://bugs.debian.org/968368)	ifenslave	ifenslave: Option bond-master fails to add interface to bond
990428 (https://bugs.debian.org/990428)	ifenslave	ifenslave: Bonding not working on bullseye (using bond-slaves config)
991113 (https://bugs.debian.org/991113)	libpam-chroot	libpam-chroot installs pam_chroot.so into the wrong directory
989545 (https://bugs.debian.org/989545)	src:llvm-toolchain-11	libgl1-mesa-dri: si_texture.c:1727 si_texture_transfer_map - failed to create temporary texture to hold untiled copy
982459 (https://bugs.debian.org/982459)	mdadm	mdadm --examine in chroot without /proc,/dev,/sys mounted corrupts host's filesystem
981054 (https://bugs.debian.org/981054)	openipmi	openipmi: Missing dependency on kmod
948318 (https://bugs.debian.org/948318)	openssh-server	openssh-server: Unable to restart sshd restart after upgrade to version 8.1p1-2
991151 (https://bugs.debian.org/991151)	procps	procps: dropped the reload option from the init script, breaking corekeeper
989103 (https://bugs.debian.org/989103)	pulseaudio	pulseaudio regressed on control=Wave configuration
984580 (https://bugs.debian.org/984580)	libpython3.9-dev	libpython3.9-dev: missing dependency on zlib1g-dev
990417 (https://bugs.debian.org/990417)	src:qemu	openjdk-11-jre-headless: running java in qemu s390 gives a SIGILL at C [linux-vdso64.so.1+0x6f8] __kernel_getcpu+0x8
859926 (https://bugs.debian.org/859926)	speech-dispatcher	breaks with pulse-audio as output when spawned by speechd-up from init system

Bug number	Package (source or binary)	Description
932501 (https://bugs.debian.org/932501)	src:squid-deb-proxy	squid-deb-proxy: daemon does not start due to the conf file not being allowed by apparmor
991588 (https://bugs.debian.org/991588)	tpm2-abrmd	tpm2-abrmd should not use Requires = systemd-udev-settle.service in its unit
991939 (https://bugs.debian.org/991939)	libjs-bootstrap4	libjs-bootstrap4: broken symlinks: /usr/share/javascript/bootstrap4/css/bootstrap*.css.map -> ../../../nodejs/bootstrap/dist/css/bootstrap*.c
991822 (https://bugs.debian.org/991822)	src:wine	src:wine: dh_auto_clean deletes unrelated files outside of package source
988477 (https://bugs.debian.org/988477)	src:xen	xen-hypervisor-4.14-amd64: xen dmesg shows (XEN) AMD-Vi: IO_PAGE_FAULT on sata pci device
991788 (https://bugs.debian.org/991788)	xfce4-settings	xfce4-settings: black screen after suspend when laptop lid is closed and re-opened

Capítulo 6

Más información sobre Debian

6.1. Para leer más

Además de estas notas de publicación y de la «Guía de Instalación», tiene a su disposición otros documentos sobre Debian en el Proyecto de Documentación de Debian («Debian Documentation Project» o DDP, N. del T.), cuyo objetivo es crear documentación de alta calidad para los usuarios y desarrolladores de Debian, como por ejemplo: la «Referencia de Debian», la «Guía de Debian para Nuevos Mantenedores», las «Preguntas Frecuentes sobre Debian» (FAQ), y muchos otros documentos. Si desea más detalles sobre los recursos disponibles consulte la página web del Proyecto de Documentación (`https://www.debian.org/doc/`) y el sitio web del Wiki de Debian (`https://wiki.debian.org/`).

La documentación para los paquetes individuales se instala en `/usr/share/doc/`*`paquete`*. Puede incluir información sobre el copyright, detalles específicos para Debian, y la documentación del autor original.

6.2. Cómo conseguir ayuda

Hay muchas fuentes de ayuda, consejo y apoyo para los usuarios de Debian, pero solo debería tenerlas en cuenta si ha agotado todos los recursos disponibles buscando documentación sobre su problema. Esta sección proporciona una breve introducción a estas fuentes que puede ser de ayuda para los nuevos usuarios de Debian.

6.2.1. Listas de correo electrónico

Las listas de correo de mayor interés para los usuarios de Debian son la lista «debian-user» (en inglés) y otras listas del tipo «debian-user-*idioma*» (para otros idiomas). En particular, para usuarios de habla española, la lista correspondiente es «debian-user-spanish». Para más información sobre estas listas y los detalles para suscribirse a ellas, visite `https://lists.debian.org/`. Busque la respuesta a su pregunta en los archivos antes de enviar una pregunta, y respete las «normas de etiqueta» estándar en las listas.

6.2.2. Internet Relay Chat (IRC)

Debian tiene un canal de IRC dedicado a la ayuda y asistencia para los usuarios de Debian situado en la red de IRC de OFTC. Si desea acceder al canal, conecte su cliente de IRC favorito a irc.debian.org y únase al canal `#debian`.

Siga las normas del canal, y respete totalmente a los otros usuarios. Puede consultar las normas en el Wiki de Debian (`https://wiki.debian.org/DebianIRC`).

Si desea más información sobre OFTC visite su sitio web (`http://www.oftc.net/`).

6.3. Cómo informar de fallos

Nos esforzamos para hacer de Debian un sistema operativo de gran calidad, pero esto no significa que los paquetes que proporcionemos estén totalmente libres de fallos. De acuerdo con la filosofía de

"desarrollo abierto" de Debian, y como un servicio a nuestros usuarios, proporcionamos toda la información de los fallos de los que se nos informa en nuestro propio sistema de seguimiento de fallos (Bug Tracking System o BTS). El BTS se puede consultar en https://bugs.debian.org/.

Si encuentra algún fallo en la distribución o en los programas empaquetados que forman parte de ella, le rogamos que nos informe para que pueda corregirse adecuadamente de cara a próximas versiones. Para informar de un fallo es necesario tener una dirección de correo válida. Pedimos esto porque así podemos rastrear los fallos y para que los desarrolladores puedan ponerse en contacto con los remitentes de los fallos en caso de que necesiten más información.

Puede enviar un informe de fallo usando el programa **reportbug** o de forma manual usando el correo electrónico. Puede leer más sobre el sistema de seguimiento de fallos y cómo utilizarlo en la documentación de referencia (disponible en /usr/share/doc/debian si ha instalado el paquete doc-debian) o en línea, accediendo al propio sistema de seguimiento de fallos (https://bugs.debian.org/).

6.4. Cómo colaborar con Debian

No tiene que ser un experto para colaborar con Debian. Puede contribuir a la comunidad ayudando a otros usuarios en las distintas listas (https://lists.debian.org/) de ayuda a los usuarios. También es sumamente útil identificar (y resolver) problemas relacionados con el desarrollo de la distribución participando en las listas de correo (https://lists.debian.org/) de desarrollo. Para mantener la distribución de alta calidad de Debian puede informar sobre fallos (https://bugs.debian.org/) y ayudar a los desarrolladores a seguirlos y arreglarlos. La herramienta how-can-i-help le ayudará a encontrar erratas reportadas en las que puede ayudar. Si tiene habilidad con las palabras, quizá quiera contribuir más activamente ayudando a escribir documentación (https://www.debian.org/doc/vcs) o a traducir (https://www.debian.org/international/) documentación ya existente a su propio idioma.

Si puede dedicar más tiempo, podría gestionar una parte de la colección de Software Libre de Debian. Es especialmente útil que se adopten o mantengan elementos que la gente ha pedido que se incluyan en Debian. La base de datos de paquetes en perspectiva o para los que se necesita ayuda (https://www.debian.org/devel/wnpp/) (Work Needing and Prospective Packages o WNPP, N. del T.) contiene todos los detalles e información al respecto. Si tiene interés en algún grupo en concreto quizás disfrute colaborando con alguno de los subproyectos (https://www.debian.org/devel/#projects) de Debian, como pueden ser la adaptación a alguna arquitectura concreta, y Debian Pure Blends (https://wiki.debian.org/DebianPureBlends) para grupos de usuario específicos, entre otros.

En cualquier caso, si ya está trabajando en la comunidad del software libre de alguna manera, como usuario, programador, escritor o traductor, ya está ayudando al esfuerzo del software libre. Colaborar es gratificante y divertido, y además de permitirle conocer nuevas personas, le hará sentirse mejor.

Capítulo 7

Glosario

ACPI

Advanced Configuration and Power Interface («Interfaz avanzada de configuración y energía», N. del T.)

ALSA

Advanced Linux Sound Architecture («Arquitectura avanzada de sonido de Linux», N. del T.)

BD

Disco Blu-ray

CD

Disco compacto

CD-ROM

Compact Disc Read Only Memory («Memoria de solo lectura de disco compacto», N. del T.)

DHCP

Dynamic Host Configuration Protocol («Protocolo de configuración dinámica de sistemas», N. del T.)

DLBD

Disco Blu-ray de doble capa

DNS

Domain Name System («Sistema de nombres de dominio», N. del T.)

DVD

Digital Versatil Disc («Disco digital versátil», N. del T.)

GIMP

Programa de Manipulación de Imágenes de GNU

GNU

GNU's Not Unix («GNU no es Unix», N. del T.)

GPG

GNU Privacy Guard

LDAP

Lightweight Directory Acccess Protocol («Protocolo ligero de acceso a directorios», N. del T.)

LSB

Linux Standard Base («Estándares base de Linux», N. del T.)

LVM

Logical Volume Manager («Administrador de volúmenes lógicos», N. del T.)

MTA

Mail Transport Agent («Agente de transporte de correo», N. del T.)

NBD

Network Block Debice («Dispositivo de bloques de red», N. del T.)

NFS

Network File System («Sistema de ficheros en red», N. del T.)

NIC

Network Interface Card («Tarjeta de red», N. del T.)

NIS

Network Information Service («Sistema de información de red», N. del T.)

PHP

PHP: Preprocesador de Hipertexto

RAID

Redundant Array of Independent Disks («Disposición redundante de discos independientes», N. del T.)

SATA

Serial Advanced Technology Attachment («Tecnología avanzada de conexiones serie», N. del T.)

SSL

Secure Sockets Layer («Capa de conexión segura», N. del T.)

TLS

Transport Layer Security («Seguridad en la capa de transporte», N. del T.)

UEFI

Unified Extensible Firmware Interface («Interfaz unificada extensible de firmware», N. del T.)

USB

Universal serial bus («Bus serie universal», N. del T.)

UUID

Universally Unique Identifier («Identificador único universal», N. del T.)

WPA

Wi-Fi Protected Access («Acceso protegido Wi-Fi», N. del T.)

Apéndice A

Gestión de su sistema buster antes de la actualización

Este apéndice contiene la información sobre cómo asegurarse de que puede instalar o actualizar los paquetes de buster antes de actualizar a bullseye. Esto solo debería ser necesario en situaciones muy concretas.

A.1. Actualizar su sistema buster

Esta tarea es básicamente como cualquier otra actualización de buster que haya realizado. La única diferencia es que primero necesita asegurarse de que su lista de paquetes contiene referencias a buster tal y como se describe en Sección A.2.

Si actualiza su sistema usando una réplica de Debian, automáticamente se actualizará a la última versión de buster.

A.2. Comprobar su lista de fuentes APT

Si existe alguna referencia en sus archivos de fuentes APT (consulte sources.list(5) (`https://manpages.debian.org//bullseye/apt/sources.list.5.html`)) contienen referencias a "`stable`", ya está utilizando bullseye. Esto puede no ser lo que Vd. desee si no está preparado aún para hacer la actualización. Si ya ha ejecutado **apt update**, todavía puede volver a atrás sin problemas siguiendo el procedimiento explicado a continuación.

Si también ha instalado los paquetes desde bullseye, probablemente ya no tiene mucho sentido instalar paquetes desde buster. En ese caso, tendrá que decidir si quiere continuar o no. Es posible instalar una versión anterior de un paquete, pero ese procedimiento no se describe aquí.

Abra el archivo (como `root`) las fuentes apropiadas de APT (como `/etc/apt/sources.list`) con su editor favorito y compruebe todas las las líneas que comiencen por `deb http:`, `deb https:`, `deb tor+http:`, `deb tor+https:`, `URIs: http:`, `URIs: https:`, `URIs: tor+http:` o `URIs: tor+https:` para ver si existe alguna referencia a "`stable`". Si encuentra alguna, cambie `stable` por `buster`.

Si existe alguna línea que comienza por `deb file:` o `URIs: file:`, tendrá que comprobar si la ubicación a la que hace referencia contiene un archivo de buster o de bullseye.

> IMPORTANTE
>
> 
>
> No cambie ninguna línea que comience por `deb cdrom:` o `URIs: cdrom:`. Hacerlo invalidaría la línea y tendría que ejecutar de nuevo **apt-cdrom**. No se preocupe si alguna línea de una fuente de `cdrom` hace referencia a "`unstable`". Puede parecer confuso, pero es normal.

Si ha realizado algún cambio, guarde el archivo y ejecute:

```
# apt update
```

para actualizar la lista de paquetes.

A.3. Borrar ficheros de configuración obsoletos

Antes de actualizar su sistema a bullseye es recomendable borrar los ficheros de configuración obsoletos (como los archivos `*.dpkg-{new,old}` que se puedan encontrar bajo el directorio `/etc` del sistema.

Apéndice B

Personas que han contribuido a estas notas de publicación

Hay muchas personas que han ayudado con estas notas de publicación, incluyendo, entre otros, a Adam D. Barratt, Adam Di Carlo, Andreas Barth, Andrei Popescu, Anne Bezemer, Bob Hilliard, Charles Plessy, Christian Perrier, Christoph Berg, Daniel Baumann, David Prévot, Eddy Petrișor, Emmanuel Kasper, Esko Arajärvi, Frans Pop, Giovanni Rapagnani, Gordon Farquharson, Hideki Yamane, Holger Wansing, Javier Fernández-Sanguino Peña, Jens Seidel, Jonas Meurer, Jonathan Nieder, Joost van Baal-Ilić, Josip Rodin, Julien Cristau, Justin B Rye, LaMont Jones, Luk Claes, Martin Michlmayr, Michael Biebl, Moritz Mühlenhoff, Niels Thykier, Noah Meyerhans, Noritada Kobayashi, Osamu Aoki, Paul Gevers, Peter Green, Rob Bradford, Samuel Thibault, Simon Bienlein, Simon Paillard, Stefan Fritsch, Steve Langasek, Steve McIntyre, Tobias Scherer, victory, Vincent McIntyre, y W. Martin Borgert.

Este documento ha sido traducido a muchos idiomas. ¡Muchas gracias a los traductores!

Traducido al español por: Ricardo Cárdenes Medina, David Martínez Moreno, Juan Manuel García Molina, Javier Fernández-Sanguino, Francisco Javier Cuadrado, Igor Támara, y Fernando González de la Requena.

Índice alfabético