Release-Notes for Debian 13 (trixie)

Debian Documentation Team

2025-07-27

Índice general

1. Introducción **3**
- 1.1. Cómo informar de fallos en este documento . . . 3
- 1.2. Cómo contribuir con informes de actualización . . . 4
- 1.3. Fuentes de este documento . . . 4

2. Las novedades de Debian 13 **5**
- 2.1. Arquitecturas soportadas . . . 5
- 2.2. ¿Qué novedades hay en la distribución? . . . 6
  - 2.2.1. Soporte oficial para riscv64 . . . 6
  - 2.2.2. Hardening against ROP and COP/JOP attacks on amd64 and arm64 . . . 6
  - 2.2.3. Soporte de HTTP Boot . . . 6
  - 2.2.4. Improved manual pages translations . . . 6
  - 2.2.5. 64-bit time_t ABI transition . . . 6
  - 2.2.6. Entornos de escritorio y paquetes conocidos . . . 7

3. Sistema de instalación **9**
- 3.1. ¿Qué hay de nuevo en el sistema de instalación? . . . 9
- 3.2. Installing Debian Pure Blends . . . 10
- 3.3. Instalaciones en la nube . . . 10
- 3.4. Imágenes para contenedores y máquinas virtuales . . . 10

4. Actualizaciones desde Debian 12 (bookworm) **11**
- 4.1. Prepararse para la actualización . . . 11
  - 4.1.1. Haga copias de seguridad de sus datos e información de configuración . . . 11
  - 4.1.2. Informar a los usuarios anticipadamente . . . 12
  - 4.1.3. Prepararse para la indisponibilidad de servicios . . . 12
  - 4.1.4. Prepararse para la recuperación . . . 12
  - 4.1.5. Preparar un entorno seguro para la actualización . . . 13
- 4.2. Comenzar de un Debian «puro» . . . 14
  - 4.2.1. Actualización a Debian 12 (bookworm) . . . 14
  - 4.2.2. Actualización a la siguiente subversión publicada . . . 14
  - 4.2.3. Debian Backports . . . 14
  - 4.2.4. Preparar la base de datos de paquetes . . . 15
  - 4.2.5. Eliminar paquetes obsoletos . . . 15
  - 4.2.6. Eliminar paquetes que no son de Debian . . . 15
  - 4.2.7. Limpieza de restos de archivos de configuración . . . 15
  - 4.2.8. Los componentes non-free y non-free-firmware . . . 15

4.2.9. La sección proposed-updates . . . 16
4.2.10. Fuentes no oficiales . . . 16
4.2.11. Desactivar el bloqueo de APT . . . 16
4.2.12. Verificar el estado de los paquetes . . . 16
4.3. Preparing APT sources files . . . 17
4.3.1. Añadir fuentes en Internet para APT . . . 17
4.3.2. Añadir las réplicas locales para APT . . . 18
4.3.3. Añadir fuentes para APT de medios ópticos . . . 18
4.4. Actualizar los paquetes . . . 19
4.4.1. Grabar la sesión . . . 19
4.4.2. Actualizar las listas de paquetes . . . 20
4.4.3. Asegúrese de que tiene suficiente espacio libre para actualizar . . . 20
4.4.4. Detener sistemas de monitoreo . . . 22
4.4.5. Actualización mínima del sistema . . . 22
4.4.6. Actualizar el sistema . . . 22
4.5. Posibles problemas durante o después de la actualización . . . 23
4.5.1. Dist-upgrade falla con «No se pudo realizar la configuración inmediata» . . . 23
4.5.2. Eliminaciones esperadas . . . 23
4.5.3. Bucles en Conflictos o Pre-Dependencias . . . 23
4.5.4. Conflictos de archivo . . . 24
4.5.5. Cambios de configuración . . . 24
4.5.6. Cambio de la sesión en consola . . . 24
4.6. Actualización de su núcleo y paquetes relacionados . . . 25
4.6.1. Instalación de un metapaquete del núcleo . . . 25
4.6.2. 64-bit little-endian PowerPC (ppc64el) page size . . . 26
4.7. Prepararse para la siguiente distribución . . . 26
4.7.1. Purgando los paquetes eliminados . . . 26
4.8. Paquetes obsoletos . . . 27
4.8.1. Paquetes «dummy» de transición . . . 27

5. Problemas a tener en cuenta para trixie **29**
5.1. Things to be aware of while upgrading to trixie . . . 29
5.1.1. Reduced support for i386 . . . 29
5.1.2. 64-bit little-endian MIPS (`mips64el`) removed . . . 30
5.1.3. The temporary-files directory /tmp is now stored in a tmpfs . . . 30
5.1.4. openssh-server ya no lee ~/.pam_environment . . . 30
5.1.5. OpenSSH ya no soporta claves DSA . . . 30
5.1.6. The last, lastb and lastlog commands have been replaced . . . 31
5.1.7. Encrypted filesystems need systemd-cryptsetup package . . . 31
5.1.8. Default encryption settings for plain-mode dm-crypt devices changed . . . 31
5.1.9. RabbitMQ ya no soporta colas (queues) HA . . . 32
5.1.10. RabbitMQ no puede ser actualizado directamente desde bookworm . . . 32
5.1.11. MariaDB major version upgrades only work reliably after a clean shutdown . . . 32
5.1.12. Ping ya no se ejecuta con privilegios elevados . . . 32
5.1.13. Dovecot configuration changes . . . 33
5.1.14. Significant changes to libvirt packaging . . . 33
5.1.15. Samba: Active Directory Domain Controller packaging changes . . . 33
5.1.16. Samba: VFS modules . . . 33
5.1.17. OpenLDAP TLS now provided by OpenSSL . . . 33
5.1.18. bacula-director: Database schema update needs large amounts of disk space and time . . . 34
5.1.19. dpkg: warning: unable to delete old directory: … . . . 34
5.1.20. Skip-upgrades are not supported . . . 34
5.1.21. WirePlumber has a new configuration system . . . 34
5.1.22. strongSwan migration to a new charon daemon . . . 34

5.1.23. Things to do before rebooting . . . 35
5.2. Elementos no limitados durante el proceso de actualización . . . 35
5.2.1. The directories /tmp and /var/tmp are now regularly cleaned . . . 35
5.2.2. systemd message: System is tainted: unmerged-bin . . . 35
5.2.3. Limitaciones en el soporte de seguridad . . . 35
5.2.4. Problems with VMs on 64-bit little-endian PowerPC (ppc64el) . . . 36
5.3. Obsolescencia y deprecación . . . 36
5.3.1. Paquetes obsoletos notables . . . 36
5.3.2. Componentes obsoletos de trixie . . . 37
5.4. Bugs graves conocidos . . . 38

6. Más información sobre Debian **39**
6.1. Para leer más . . . 39
6.2. Cómo conseguir ayuda . . . 39
6.2.1. Listas de correo electrónico . . . 39
6.2.2. Internet Relay Chat (IRC) . . . 40
6.3. Cómo informar de fallos . . . 40
6.4. Cómo colaborar con Debian . . . 40

7. Gestión de su sistema bookworm antes de la actualización **41**
7.1. Actualizar su sistema bookworm . . . 41
7.2. Checking your APT configuration . . . 41
7.3. Realizando la actualización a la última versión de bookworm . . . 42
7.4. Borrar ficheros de configuración obsoletos . . . 42

8. Personas que han contribuido a estas notas de publicación **43**

El Proyecto de Documentación de Debian <https://www.debian.org/doc>.

Última actualización: 2025-07-27

CAPÍTULO 1

Introducción

Este documento informa a los usuarios de la distribución Debian sobre los cambios más importantes de la versión 13 (nombre en clave «trixie»).

Las notas de publicación proporcionan la información sobre cómo actualizar de una forma segura desde la versión 12 (nombre en clave bookworm) 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/trixie/releasenotes.

Prudencia: 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 bookworm). Si necesita actualizar su sistema desde una versión más antigua, le sugerimos que primero actualice a la versión bookworm 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 contra el paquete **release-notes**. Puede que desee revisar primero los informes de erratas existentes 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 *Sources for this document*.

1.2 Cómo contribuir con informes de actualización

Agradecemos cualquier información que los usuarios quieran proporcionar relacionada con las actualizaciones desde la versión bookworm a la versión trixie. Si está dispuesto a compartir la información, por favor mande un informe de fallo al sistema de seguimiento de fallos. 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 <systemitem role=»package»>apt</systemitem> (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 *Haga copias de seguridad de sus datos e información de configuración*, 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 *Grabar la sesión*.
- 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 reStructuredText, utilizando el conversor sphinx. La versión HTML se genera utilizando *sphinx-build -b html*. La versión PDF se genera utilizando *sphinx-build -b latex*. 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 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 para más información sobre cómo acceder al repositorio Git.

CAPÍTULO 2

Las novedades de Debian 13

La Wiki tiene más información sobre este tema.

2.1 Arquitecturas soportadas

Las siguientes son las arquitecturas oficialmente soportadas en Debian 13:

- 64-bit PC (`amd64`)
- 64-bit ARM (`arm64`)
- ARM EABI (`armel`)
- ARMv7 (EABI hard-float ABI, `armhf`)
- 64-bit little-endian PowerPC (`ppc64el`)
- 64-bit little-endian RISC-V (`riscv64`)
- IBM System z (`s390x`)

Additionally, on 64-bit PC systems, a partial 32-bit userland (`i386`) is available. Please see *Reduced support for i386* for details.

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.

2.2 ¿Qué novedades hay en la distribución?

2.2.1 Soporte oficial para riscv64

Esta versión por primera vez soporta oficialmente la arquitectura riscv64, permitiendo a los usuarios ejecutar Debian en hardware RISC-V de 64 bits y beneficiarse de todas las características de Debian 13.

La Wiki proporciona más detalles sobre el soporte de riscv64 en Debian.

2.2.2 Hardening against ROP and COP/JOP attacks on amd64 and arm64

trixie introduces security features on the amd64 and arm64 architectures designed to mitigate Return-Oriented Programming (ROP) exploits and Call/Jump-Oriented Programming (COP/JOP) attacks.

On amd64 this is based on Intel Control-flow Enforcement Technology (CET) for both ROP and COP/JOP protection, on arm64 it is based on Pointer Authentication (PAC) for ROP protection and Branch Target Identification (BTI) for COP/JOP protection.

The features are enabled automatically if your hardware supports them. For amd64 see the Linux kernel documentation and the Intel documentation, and for arm64 see the Wiki, and the Arm documentation, which have information on how to check if your processor supports CET and PAC/BTI and how they work.

2.2.3 Soporte de HTTP Boot

El Debian Installer y las Debian Live Images ahora pueden ser arrancadas usando «HTTP Boot» en firmware UEFI y U-Boot compatible.

En sistemas que usan firmware TianoCore, entre al menú *Device Manager*, luego elija *Network Device List*, seleccione la interfaz de red, *HTTP Boot Configuration*, y especifique la URL completa a la ISO de Debian a arrancar.

Para otras implementaciones de firmware, por favor vea la documentación del hardware de su sistema y/o la documentación del firmware.

2.2.4 Improved manual pages translations

The *manpages-l10n* project has contributed many improved and new translations for manual pages. Especially Romanian and Polish translations are greatly enhanced since bookworm.

2.2.5 64-bit time_t ABI transition

All architectures other than `i386` now use a 64-bit `time_t` ABI, supporting dates beyond 2038.

On 32-bit architectures (`armel` and `armhf`) the ABI of many libraries changed without changing the library «soname». On these architectures, third-party software and packages will need to be recompiled/rebuilt, and checked for possibly silent data loss.

The `i386` architecture did not participate in this transition, since its primary function is to support legacy software.

More details can be found on the Debian wiki.

2.2.6 Entornos de escritorio y paquetes conocidos

This new release of Debian comes with a lot more software than its predecessor bookworm; the distribution includes over 11294 new packages, for a total of over 59551 packages. Most of the software in the distribution has been updated: over 42821 software packages (this is 72 % of all packages in bookworm). Also, a significant number of packages (over 9519, 16 % of the packages in bookworm) have for various reasons been removed from the distribution. You will not see any updates for these packages and they will be marked as «obsolete» in package management front-ends; see *Paquetes obsoletos*.

Debian again ships with several desktop applications and environments. Among others it now includes the desktop environments GNOME 48, KDE Plasma 6.3, LXDE 13, LXQt 2.1.0, and Xfce 4.20.

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

- LibreOffice is upgraded to version 25;
- GNUcash is upgraded to 5.10;

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

Paquete	Versión en 12 (bookworm)	Versión en 13 (trixie)
Apache	2.4.62	2.4.64
Bash	5.2.15	5.2.37
Servidor DNS BIND	9.18	9.20
Cryptsetup	2.6	2.7
Emacs	28.2	30.1
Exim (default email server)	4.96	4.98
GCC, the GNU Compiler Collection (default compiler)	12.2	14.2
GIMP	2.10.34	3.0.4
GnuPG	2.2.40	2.4.7
Inkscape	1.2.2	1.4
la biblioteca C de GNU	2.36	2.41
Linux kernel	6.1 series	6.12 series
LLVM/Clang toolchain	13.0.1 and 14.0 (default) and 15.0.6	19 (default), 17 and 18 available
MariaDB	10.11	11.8
Nginx	1.22	1.26
OpenJDK	17	21
OpenLDAP	2.5.13	2.6.10
OpenSSH	9.2p1	10.0p1
OpenSSL	3.0	3.5
Perl	5.36	5.40
PHP	8.2	8.4
Postfix	3.7	3.10
PostgreSQL	15	17
Python 3	3.11	3.13
Rustc	1.63	1.85
Samba	4.17	4.22
Systemd	252	257
Vim	9.0	9.1

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 trixie junto con la Guía de instalación en la página web de Debian (https://www.debian.org/releases/trixie/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/language/index.html
```

Quizás también quiera consultar la página de errata disponible en https://www.debian.org/releases/trixie/debian-installer#errata para conocer los problemas conocidos.

3.1 ¿Qué hay de nuevo en el sistema de instalación?

Se ha realizado mucho desarrollo en el instalador de Debian desde su primera versión oficial en Debian 12, 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 bookworm, consulte los anuncios de publicación de las versiones beta y RC de trixie disponibles en el histórico de noticias del instalador de Debian.

3.2 Installing Debian Pure Blends

A selection of Debian Pure Blends, such as Debian Junior, Debian Science, or Debian FreedomBox, can now be accessed directly in the installer - see the installation-guide.

For information about Debian Pure Blends, visit https://www.debian.org/blends/ or the wiki.

3.3 Instalaciones en la nube

El equipo de la nube publica Debian bullseye para varios servicios de computación en la nube populares incluyendo:

- Amazon Web Services
- Microsoft Azure
- OpenStack
- Máquina virtual normal

Las imágenes para la nube incluyen ganchos de automatización a través de `cloud-init` y priorizan el arranque rápido de la imagen utilizando paquetes optimizados del núcleo y configuraciones de grub. Se proporcionan imágenes dando soporte a distintas arquitecturas cuando se considera necesario y el equipo de la nube se esfuerza en proporcionar soporte a todas las funcionalidades que ofrece el servicio en la nube.

The cloud team will provide updated images until the end of the LTS period for trixie. New images are typically released for each point release and after security fixes for critical packages. The cloud team's full support policy is available on the Cloud Image Lifecycle page.

Puede encontrar más información en https://cloud.debian.org/ y en el wiki.

3.4 Imágenes para contenedores y máquinas virtuales

Hay disponibles imágenes de contenedor multi-arquitectura de Debian trixie en Docker Hub. Existe una variante «slim» (N. del T. «delgada») que reduce el espacio en disco además de las imágenes estándar.

CAPÍTULO 4

Actualizaciones desde Debian 12 (bookworm)

4.1 Prepararse para la actualización

Sugerimos que antes de actualizar también lea la información en *Problemas a tener en cuenta para trixie*. Ese capítulo cubre problemas potenciales que no están directamente relacionados con el proceso de actualización pero que aún podrían ser importantes conocer antes de comenzar.

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.

Las principales cosas que querrá respaldar son los contenidos de `/etc`, `/var/lib/dpkg`, `/var/lib/apt/extended_states` y la salida de:

```
$ dpkg --get-selections '*' # (the quotes are important)
```

Si usa `aptitude` para gestionar paquetes en su sistema, también querrá respaldar `/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 trixie, 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 se está actualizando proporciona servicios críticos para sus usuarios o la red[2], puede reducir el tiempo de inactividad si hace una actualización mínima del sistema, como se describe en *Minimal system upgrade*, seguida de una actualización del núcleo y reinicio, y luego actualizar los paquetes asociados con sus servicios críticos. Actualice estos paquetes antes de hacer la actualización completa descrita en *Upgrading the system*. De esta manera puede asegurar que estos servicios críticos estén ejecutándose y disponibles a través del proceso de actualización completa, y su tiempo de inactividad se reduzca.

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 recuperación de emergencia generalmente recomendamos usar el *modo de rescate* del Debian Installer de trixie. La ventaja de usar el instalador es que puede elegir entre sus muchos métodos para encontrar uno que mejor se adapte a su situación. Para más información, por favor consulte la sección «Recovering a Broken System» en el capítulo 8 de la Guía de Instalación (en https://www.debian.org/releases/trixie/installmanual) y las Debian Installer FAQ.

[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.

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 («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.

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 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.

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 /
```

Otro enfoque es habilitar el «early debug shell» de systemd a través del `debug-shell.service`. En el siguiente arranque este servicio abre un shell de inicio de sesión de root en tty9 muy temprano en el proceso de arranque. Se puede habilitar con el parámetro de arranque del núcleo `systemd.debug-shell=1`, o hacerlo persistente con `systemctl enable debug-shell` (en cuyo caso debería deshabilitarse nuevamente cuando se complete la depuración).

Puede encontrar más información de la depuración de un sistema de arranque con problemas bajo systemd en el artículo Diagnosticando problemas de arranque.

4.1.5 Preparar un entorno seguro para la actualización

Importante: Si está usando algunos servicios VPN (como **tinc**) considere que podrían no estar disponibles durante todo el proceso de actualización. Por favor vea *Prepare for downtime on services*.

In order to gain extra safety margin when upgrading remotely, we suggest that you run upgrade processes in a virtual console provided by the `screen` or `tmux` programs, which enables safe reconnection and ensures the upgrade process is not interrupted even if the remote connection process temporarily fails.

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

Los usuarios del daemon de watchdog proporcionado por el paquete **micro-evtd** deberían detener el daemon y deshabilitar el temporizador de watchdog antes de la actualización, para evitar un reinicio inesperado en el medio 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 bookworm 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.

APT is moving to a different format for configuring where it downloads packages from. The files `/etc/apt/sources.list` and `*.list` files in `/etc/apt/sources.list.d/` are replaced by files still in that directory but with names ending in `.sources`, using the new, more readable (deb822 style) format. For details see sources.list(5). Examples of APT configurations in these notes will be given in the new deb822 format.

If your system is using multiple sources files then you will need to ensure they stay consistent.

4.2.1 Actualización a Debian 12 (bookworm)

No se proporciona soporte a las actualizaciones directas de versiones de Debian más antiguas que 12 (bookworm). Puede mostrar su versión de Debian ejecutando:

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

Por favor, siga las instrucciones en las Notas de publicación para Debian (https://www.debian.org/releases/bookworm/releasenotes) para actualizarse primero a Debian 12.

4.2.2 Actualización a la siguiente subversión publicada

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

4.2.3 Debian Backports

Debian Backports permite a los usuarios de Debian stable ejecutar versiones más actualizadas de paquetes (con algunos compromisos en el soporte de pruebas y seguridad). El Equipo de Debian Backports mantiene un subconjunto de paquetes de la siguiente versión de Debian, ajustados y recompilados para uso en la versión stable actual de Debian.

Los paquetes de bookworm-backports tienen números de versión menores que la versión en trixie, así que deberían actualizar normalmente a trixie de la misma manera que los paquetes «puros» de bookworm durante la actualización de distribución. Aunque no hay problemas potenciales conocidos, las rutas de actualización desde backports están menos probadas, y en consecuencia incurren en más riesgo.

Prudencia: While regular Debian Backports are supported, there is no clean upgrade path from sloppy backports (which use APT sources entries referencing bookworm-backports-sloppy).

As with *Unofficial sources*, users are advised to remove «bookworm-backports» entries from their APT sources files before the upgrade. After it is completed, they may consider adding «trixie-backports» (see https://backports.debian.org/Instructions/).

Para más información, consulte la página Wiki de Backports.

4.2.4 Preparar la base de datos de paquetes

You should make sure the package database is ready before proceeding with the upgrade. If you are a user of another package manager like **aptitude** or **synaptic**, review any pending actions. A package scheduled for installation or removal might interfere with the upgrade procedure. Note that correcting this is only possible if your APT sources files still point to «bookworm» and not to «stable» or «trixie»; see *Checking your APT configuration*.

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 Eliminar paquetes que no son de Debian

A continuación hay dos métodos para encontrar paquetes instalados que no vinieron de Debian, usando ya sea `apt` o `apt-forktracer`. Por favor tenga en cuenta que ninguno de ellos es 100 % exacto (p. ej. el ejemplo de apt listará paquetes que una vez fueron proporcionados por Debian pero ya no lo son, como paquetes de núcleo antiguos).

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

4.2.7 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'
```

4.2.8 Los componentes non-free y non-free-firmware

If you have non-free firmware installed it is recommended to add `non-free-firmware` to your APT sources.

4.2.9 La sección proposed-updates

If you have listed the `proposed-updates` section in your APT sources files, you should remove it before attempting to upgrade your system. This is a precaution to reduce the likelihood of conflicts.

4.2.10 Fuentes no oficiales

If you have any non-Debian packages on your system, you should be aware that these may be removed during the upgrade because of conflicting dependencies. If these packages were installed by adding an extra package archive in your APT sources files, you should check if that archive also offers packages compiled for trixie and change the source item accordingly at the same time as your source items for Debian packages.

Algunos usuarios pueden tener versiones «más nuevas» *no oficiales* retroportadas de paquetes que *están* en Debian instalados en su sistema bookworm. Tales paquetes tienen más probabilidades de causar problemas durante una actualización ya que pueden resultar en conflictos de archivos[4]. *Possible issues during upgrade* tiene alguna información sobre cómo manejar conflictos de archivos si llegaran a ocurrir.

4.2.11 Desactivar el bloqueo de APT

Si ha configurado APT para instalar ciertos paquetes de una distribución distinta de stable (p. ej. de testing), puede tener que cambiar su configuración de anclaje de APT (almacenada en `/etc/apt/preferences` y `/etc/apt/preferences.d/`) para permitir la actualización de paquetes a las versiones en la nueva versión stable. Información adicional sobre el anclaje de APT se puede encontrar en apt_preferences(5).

4.2.12 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
```

o

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

Alternativamente también puede usar `apt`.

```
# apt list --installed > ~/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.

```
$ apt-mark showhold
```

[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 cambió y recompiló un paquete localmente, y no lo renombró ni puso una época en la versión, debe retenerlo para prevenir que sea actualizado.

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

```
# apt-mark hold package_name
```

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

If there is anything you need to fix, it is best to make sure your APT sources files still refer to bookworm as explained in *Checking your APT configuration*.

4.3 Preparing APT sources files

Before starting the upgrade you must reconfigure APT to add sources for trixie and typically remove sources for bookworm.

As mentioned in *Comenzar de un Debian «puro»*, we recommend that you use the new deb822-style format, so you would have to replace `/etc/apt/sources.list` and any `*.list` files in `/etc/apt/sources.list.d/` by only one file named `debian.sources` in `/etc/apt/sources.list.d/` (if you haven't done so already). An example is given below of how this file should typically look.

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 «bookworm», «trixie») 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, recibirá una notificación cada vez que se publique una nueva versión en Debian. Como por ejemplo cuando «trixie» cambie de ser, p.ej., «testing» a «stable».
- Si se subscribe a la lista de distribución de avisos de seguridad de Debian, 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.

To make use of the CDN service, the correct configuration for APT (assuming you are using `main` and `non-free-firmware`) is the following in `/etc/apt/sources.list.d/debian.sources`:

```
Types: deb
URIs: https://deb.debian.org/debian
Suites: trixie trixie-updates
```

```
Components: main non-free-firmware
Signed-By: /usr/share/keyrings/debian-archive-keyring.gpg

Types: deb
URIs: https://security.debian.org/debian\unhbox\voidb@x\kern\z@\char‘\protect\
discretionary{\char\defaulthyphenchar}{}{}security
Suites: trixie-security
Components: main non-free-firmware
Signed-By: /usr/share/keyrings/debian-archive-keyring.gpg
```

Make sure to remove any of the old sources files.

However, if you get better results using a specific mirror that is close to you in network terms instead of the CDN service, then the mirror URI can be substituted in the URIs line as (for instance) «URIs: https://mirrors.kernel.org/debian».

If you want to use packages from the `contrib` or `non-free` components, you may add these names to all the `Components:` lines.

After adding your new sources, disable the previously existing archive entries in the APT sources files by placing a hash sign (`#`) in front of them.

4.3.2 Añadir las réplicas locales para APT

Instead of using remote package mirrors, you may wish to modify the APT sources files to use a mirror on a local disk (possibly mounted over NFS).

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

```
/var/local/debian/dists/trixie/main/...
/var/local/debian/dists/trixie/contrib/...
```

To use this with **apt**, add the following to your `/etc/apt/sources.list.d/debian.sources` file:

```
Types: deb
URIs: file:/var/local/debian
Suites: trixie
Components: main non-free-firmware
Signed-By: /usr/share/keyrings/debian-archive-keyring.gpg
```

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

4.3.3 Añadir fuentes para APT de medios ópticos

If you want to use *only* DVDs (or CDs or Blu-ray Discs), comment out the existing entries in all the APT sources files by placing a hash sign (`#`) in front of them.

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    # this will mount the CD to the mount point
# ls -alF /media/cdrom  # this should show the CD's root directory
# umount /media/cdrom   # this will unmount the 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 /mountpoint
```

Next you should double-check that the APT sources entries (in files under `/etc/apt/sources.list.d/`) refer either to «trixie» or to «stable». There should not be any sources entries pointing to bookworm.

Nota: Sources lines for a CD-ROM might sometimes refer to «`unstable`»; although this may be confusing, you should *not* change it.

4.4.1 Grabar la sesión

`apt` will log the changed package states in `/var/log/apt/history.log` and the terminal output in `/var/log/apt/term.log`. `dpkg` will, in addition, log all package state changes in `/var/log/dpkg.log`. If you use `aptitude`, it will also log state changes in `/var/log/aptitude`.

If a problem occurs, you will have a log of what happened, and if needed, can provide exact information in a bug report.

The `term.log` will also allow you to review information that has scrolled off-screen. If you are at the system's console, just switch to VT2 (using `Alt+F2`) to review it.

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
```

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 *Upgrading the system*. 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 upgraded, XXX newly installed, XXX to remove and XXX not upgraded.
Need to get xx.xMB of archives.
After this operation, AAAMB of additional disk space will be used.
```

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 *Minimal system upgrade* 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: You don't have enough free space in /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 bookworm, 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 autoremove
  ```

  You can also use `debfoster` to find redundant packages. Do not blindly remove the packages this tool presents, especially if you are using aggressive non-default options that are prone to false positives. It is highly recom-

mended that you manually review the packages suggested for removal (i.e. their contents, sizes, and descriptions) before you remove them.

- 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.

- Haga una actualización mínima del sistema (vea *Minimal system upgrade*) o actualizaciones parciales del sistema seguidas de una actualización completa. Esto hará posible actualizar el sistema parcialmente, y le permitirá limpiar la caché de paquetes antes de la actualización completa.

Note that in order to safely remove packages, it is advisable to switch your APT sources files back to bookworm as described in *Checking your APT configuration*.

4.4.4 Detener sistemas de monitoreo

Como `apt` puede necesitar detener temporalmente servicios ejecutándose en su computadora, probablemente sea una buena idea detener servicios de monitoreo que pueden reiniciar otros servicios finalizados durante la actualización. En Debian, **monit** es un ejemplo de tal servicio.

4.4.5 Actualización mínima del sistema

En algunos casos, hacer la actualización completa (como se describe abajo) directamente podría eliminar grandes números de paquetes que querrá conservar. Por lo tanto recomendamos un proceso de actualización de dos partes: primero una actualización mínima para superar estos conflictos, luego una actualización completa como se describe en *Upgrading the system*.

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

4.4.6 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 trixie.

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: Could not perform immediate configuration on 'package'.  Please see man 5 apt.conf␣
↪under APT::Immediate-Configure for details.
```

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

Another possible workaround for this problem is to temporarily add both bookworm and trixie sources to your APT sources files and run `apt update`.

4.5.2 Eliminaciones esperadas

El proceso de actualización a trixie 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 trixie en *Obsolete packages*.

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 package_name
```

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 /path/to/package_name.deb
```

4.5.4 Conflictos de archivo

No deberían producirse conflictos entre archivos si actualiza de un sistema bookworm «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:

```
Unpacking <package-foo> (from <package-foo-file>) ...
dpkg: error processing <package-foo> (--install):
trying to overwrite `<some-file-name>',
which is also in package <package-bar>
dpkg-deb: subprocess paste killed by signal (Broken pipe)
Errors were encountered while processing:
<package-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 package_name
```

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 bookworm a trixie, 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 *Things to do before rebooting* 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, 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 *Minimal system upgrade*.

4.6.2 64-bit little-endian PowerPC (ppc64el) page size

From trixie, the default Linux kernel for the ppc64el architecture (package **linux-image-powerpc64le**) uses a memory page size of 4 kiB instead of the previous 64 kiB. This matches other common architectures and avoids some incompatibilities with the larger page size in the kernel (notably the `nouveau` and `xe` drivers) and user-space applications. In general this is expected to reduce memory usage and slightly increase CPU usage.

An alternate kernel package (**linux-image-powerpc64le-64k**) is provided which uses a page size of 64 kiB. You will need to install this alternate package if:

- You need to run virtual machines with a page size of 64 kiB.

  Also see *Problems with VMs on 64-bit little-endian PowerPC (ppc64el)*.

- You need to use PowerPC Nest (NX) compression.
- You are using filesystems with a block size > 4 kiB (4096 bytes). This is likely if you are using Btrfs. You can check this with:
  - Btrfs: `file -s device | grep -o 'sectorsize [0-9]*'`
  - ext4: `tune2fs -l device | grep '^Block size:'`
  - XFS: `xfs_info device | grep -o 'bsize=[0-9]*`

For some applications such as database servers, using a page size of 64 kiB can provide better performance, and this alternate kernel package may be preferable to the default.

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 nuevos redundantes u obsoletos tal y como se describe en *Make sure you have sufficient space for the upgrade* y *Obsolete packages*. Debería revisar qué archivos de configuración utilizan y considerar como opción purgarlos para eliminar sus archivos de configuración. También puede consultar la sección *Purging removed packages*.

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 bookworm) o eran parte de paquetes de terceros. Se han dado muchos casos en los que los programas de init.d antiguos han causado problemas.

Prudencia: 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):

```
$ apt list '~c'
```

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 '~c'
```

4.8 Paquetes obsoletos

La versión trixie, aunque introduce muchos paquetes nuevos, también retira o deja de distribuir algunos paquetes que estaban disponibles en bookworm. 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 trixie[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 trixie debido a los errores que presentan. En este último caso los paquetes puede que sigan estando presentes en la distribución «unstable».

Los «Paquetes Obsoletos y Creados Localmente» pueden ser listados y purgados desde la línea de comandos con:

```
$ apt list '~o'
# apt purge '~o'
```

A menudo podrá encontrar más información de por qué un paquete fue eliminado en el Sistema de seguimiento de fallos de Debian. Debería consultar tanto los informes de fallos del propio paquete como los informes de fallos archivados del pseudo-paquete ftp.debian.org.

Puede consultar una lista de los paquetes obsoletos de trixie en *Paquetes obsoletos notables*.

4.8.1 Paquetes «dummy» de transición

Algunos de los paquetes de bookworm 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.

The package descriptions for transitional dummy packages usually indicate their purpose. However, they are not uniform; in particular, some «dummy» packages are designed to be kept installed, in order to pull in a full software suite, or track the current latest version of some program.

[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.

CAPÍTULO 5

Problemas a tener en cuenta para trixie

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 *Para leer más*.

5.1 Things to be aware of while upgrading to trixie

Esta sección cubre los elementos relacionados con la actualización de bookworm a trixie.

5.1.1 Reduced support for i386

From trixie, i386 is no longer supported as a regular architecture: there is no official kernel and no Debian installer for i386 systems. Fewer packages are available for i386 because many projects no longer support it. The architecture's sole remaining purpose is to support running legacy code, for example, by way of multiarch or a chroot on a 64-bit (amd64) system.

The i386 architecture is now only intended to be used on a 64-bit (amd64) CPU. Its instruction set requirements include SSE2 support, so it will not run successfully on most of the 32-bit CPU types that were supported by Debian 12.

Los usuarios que ejecuten sistemas i386 no deberían actualizar a trixie. En su lugar, Debian recomienda reinstalarlos como amd64, donde sea posible, o retirar el hardware. El Cross-grading sin reinstalar es una alternativa técnicamente posible, pero arriesgada.

5.1.2 64-bit little-endian MIPS (mips64el) removed

From trixie, mips64el is no longer supported by Debian.

5.1.3 The temporary-files directory /tmp is now stored in a tmpfs

From trixie, the default is for the /tmp/ directory to be stored in memory using a tmpfs(5) filesystem. This should make applications using temporary files faster, but if you put large files there, you may run out of memory.

For systems upgraded from bookworm, the new behavior only starts after a reboot. Files left in /tmp will be hidden after the new *tmpfs* is mounted which will lead to warnings in the system journal or syslog. Such files can be accessed using a bind-mount (see mount(1)): running mount --bind / /mnt will make the underlying directory accessible at /mnt/tmp (run umount /mnt once you have cleaned up the old files).

The default is to allocate up to 50 % of memory to /tmp (this is a maximum: memory is only used when files are actually created in /tmp). You can change the size by running systemctl edit tmp.mount as root and setting, for example:

```
[Mount]
Options=mode=1777,nosuid,nodev,size=2G
```

(see systemd.mount(5)).

You can return to /tmp being a regular directory by running systemctl mask tmp.mount as root and rebooting.

The new filesystem defaults can also be overridden in /etc/fstab, so systems that already define a separate /tmp partition will be unaffected.

5.1.4 openssh-server ya no lee ~/.pam_environment

El daemon de Secure Shell (SSH) proporcionado en el paquete **openssh-server**, que permite inicios de sesión desde sistemas remotos, ya no lee el archivo ~/.pam_environment del usuario por defecto; esta característica tiene un historial de problemas de seguridad y ha sido obsoleta en las versiones actuales de la biblioteca Pluggable Authentication Modules (PAM). Si usaba esta característica, debería cambiar de establecer variables en ~/.pam_environment a establecerlas en sus archivos de inicialización del shell (p. ej. ~/.bash_profile o ~/.bashrc) o algún otro mecanismo similar en su lugar.

Las conexiones SSH existentes no se verán afectadas, pero las nuevas conexiones pueden comportarse de manera diferente después de la actualización. Si está actualizando remotamente, normalmente es una buena idea asegurarse de que tiene alguna otra forma de iniciar sesión en el sistema antes de iniciar la actualización; vea *Prepararse para la recuperación*.

5.1.5 OpenSSH ya no soporta claves DSA

Las claves del Algoritmo de Firma Digital (DSA), como se especifica en el protocolo de Secure Shell (SSH), son inherentemente débiles: están limitadas a claves privadas de 160 bits y el resumen SHA-1. La implementación SSH proporcionada por los paquetes **openssh-client** y **openssh-server** ha deshabilitado el soporte para claves DSA por defecto desde OpenSSH 7.0p1 en 2015, liberado con Debian 9 («stretch»), aunque aún podía habilitarse usando las opciones de configuración HostKeyAlgorithms y PubkeyAcceptedAlgorithms para claves de host y de usuario respectivamente.

Los únicos usos restantes de DSA en este punto deberían ser conectarse a algunos dispositivos muy antiguos. Para todos los demás propósitos, los otros tipos de claves soportados por OpenSSH (RSA, ECDSA y Ed25519) son superiores.

A partir de OpenSSH 9.8p1 en trixie, las claves DSA ya no están soportadas ni siquiera con las opciones de configuración mencionadas anteriormente. Si tiene un dispositivo al que solo puede conectarse usando DSA, entonces puede usar el comando `ssh1` proporcionado por el paquete **openssh-client-ssh1** para hacerlo.

En el caso improbable de que aún esté usando claves DSA para conectarse a un servidor Debian (si no está seguro, puede verificarlo agregando la opción `-v` a la línea de comandos `ssh` que usa para conectarse a ese servidor y buscar la línea «Server accepts key:»), entonces debe generar claves de reemplazo antes de actualizar. Por ejemplo, para generar una nueva clave Ed25519 y habilitar inicios de sesión a un servidor usándola, ejecute esto en el cliente, reemplazando `username@server` con los nombres de usuario y host apropiados:

```
$ ssh-keygen -t ed25519
$ ssh-copy-id username@server
```

5.1.6 The last, lastb and lastlog commands have been replaced

The **util-linux** package no longer provides the `last` or `lastb` commands, and the **login** package no longer provides `lastlog`. These commands provided information about previous login attempts using `/var/log/wtmp`, `/var/log/btmp`, `/var/run/utmp` and `/var/log/lastlog`, but these files will not be usable after 2038 because they do not allocate enough space to store the login time (the Year 2038 Problem), and the upstream developers do not want to change the file formats. Most users will not need to replace these commands with anything, but the **util-linux** package provides a `lslogins` command which can tell you when accounts were last used.

There are two direct replacements available: `last` can be replaced by `wtmpdb` from the **wtmpdb** package (the **libpam-wtmpdb** package also needs to be installed) and `lastlog` can be replaced by `lastlog2` from the **lastlog2** package (**libpam-lastlog2** also needs to be installed). If you want to use these, you will need to install the new packages after the upgrade, see the util-linux NEWS.Debian for further information. The command `lslogins --failed` provides similar information to `lastb`.

If you do not install **wtmpdb** then we recommend you remove old log files `/var/log/wtmp*`. If you do install **wtmpdb** it will upgrade `/var/log/wtmp` and you can read older wtmp files with `wtmpdb import -f <dest>`. There is no tool to read `/var/log/lastlog*` or `/var/log/btmp*` files: they can be deleted after the upgrade.

5.1.7 Encrypted filesystems need systemd-cryptsetup package

Support for automatically discovering and mounting encrypted filesystems has been moved into the new **systemd-cryptsetup** package. This new package is recommended by **systemd** so should be installed automatically on upgrades.

Please make sure the **systemd-cryptsetup** package is installed before rebooting, if you use encrypted filesystems.

5.1.8 Default encryption settings for plain-mode dm-crypt devices changed

The default settings for `dm-crypt` devices created using `plain`-mode encryption (see crypttab(5)) have changed to improve security. This will cause problems if you did not record the settings used in `/etc/crypttab`. The recommended way to configure plain-mode devices is to record the options `cipher`, `size`, and `hash` in `/etc/crypttab`; otherwise `cryptsetup` will use default values, and the defaults for cipher and hash algorithm have changed in trixie, which will cause such devices to appear as random data until they are properly configured.

This does not apply to LUKS devices because LUKS records the settings in the device itself.

To properly configure your plain-mode devices, assuming they were created with the bookworm defaults, you should add `cipher=aes-cbc-essiv:sha256,size=256,hash=ripemd160` to `/etc/crypttab`.

To access such devices with `cryptsetup` on the command line you can use `--cipher aes-cbc-essiv:sha256 --key-size 256 --hash ripemd160`. Debian recommends that you configure permanent devices with LUKS, or

if you do use plain mode, that you explicitly record all the required encryption settings in `/etc/crypttab`. The new defaults are `cipher=aes-xts-plain64` and `hash=sha256`.

5.1.9 RabbitMQ ya no soporta colas (queues) HA

Las colas de alta disponibilidad (HA) ya no están soportadas por **rabbitmq-server** a partir de trixie. Para continuar con una configuración HA, estas colas necesitan cambiarse a «quorum queues».

Si tiene un despliegue de OpenStack, por favor cambie las colas a quorum antes de actualizar. Tenga en cuenta también que comenzando con la versión «Caracal» de OpenStack en trixie, OpenStack soporta solo quorum queues.

5.1.10 RabbitMQ no puede ser actualizado directamente desde bookworm

No hay una ruta de actualización directa y fácil para RabbitMQ desde bookworm a trixie. Los detalles sobre este problema se pueden encontrar en el bug 1100165.

La ruta de actualización recomendada es limpiar completamente la base de datos de rabbitmq y reiniciar el servicio (después de la actualización a trixie). Esto puede hacerse eliminando `/var/lib/rabbitmq/mnesia` y todo su contenido.

5.1.11 MariaDB major version upgrades only work reliably after a clean shutdown

MariaDB does not support error recovery across major versions. For example if a MariaDB 10.11 server experienced an abrupt shutdown due to power loss or software defect, the database needs to be restarted with the same MariaDB 10.11 binaries so it can do successful error recovery and reconcile the data files and log files to roll-forward or revert transactions that got interrupted.

If you attempt to do crash recovery with MariaDB 11.8 using the data directory from a crashed MariaDB 10.11 instance, the newer MariaDB server will refuse to start.

To ensure a MariaDB Server is shut down cleanly before going into major version upgrade, stop the service with

```
# service mariadb stop
```

followed by checking server logs for `Shutdown complete` to confirm that flushing all data and buffers to disk completed successfully.

If it didn't shut down cleanly, restart it to trigger crash recovery, wait, stop again and verify that second stop was clean.

For additional information about how to make backups and other relevant information for system administrators, please see /usr/share/doc/mariadb-server/README.Debian.gz.

5.1.12 Ping ya no se ejecuta con privilegios elevados

The default version of ping (provided by **iputils-ping**) is no longer installed with access to the *CAP_NET_RAW* linux capability, but instead uses `ICMP_PROTO` datagram sockets for network communication. Access to these sockets is controlled based on the user's Unix group membership using the `net.ipv4.ping_group_range` sysctl. In normal installations, the **linux-sysctl-defaults** package will set this value to a broadly permissive value, allowing unprivileged users to use ping as expected, but some upgrade scenarios may not automatically install this package. See `/usr/lib/sysctl.d/50-default.conf` and the kernel documentation for more information on the semantics of this variable.

5.1.13 Dovecot configuration changes

The **dovecot** email server suite in trixie uses a configuration format that is incompatible with previous versions. Details about the configuration changes are available at docs.dovecot.org.

In order to avoid potentially extended downtime, you are strongly encouraged to port your configuration in a staging environment before beginning the upgrade of a production mail system.

Please also note that some features were removed upstream in v2.4. In particular, the *replicator* is gone. If you depend on that feature, it is advisable not to upgrade to trixie until you have found an alternative.

5.1.14 Significant changes to libvirt packaging

The **libvirt-daemon** package, which provides an API and toolkit for managing virtualization platforms, has been overhauled in trixie. Each driver and storage backend now comes in a separate binary package, which enables much greater flexibility.

Care is taken during upgrades from bookworm to retain the existing set of components, but in some cases functionality might end up being temporarily lost. We recommend that you carefully review the list of installed binary packages after upgrading to ensure that all the expected ones are present; this is also a great time to consider uninstalling unwanted components.

In addition, some conffiles might end up marked as «obsolete» after the upgrade. The `/usr/share/doc/libvirt-common/NEWS.Debian.gz` file contains additional information on how to verify whether your system is affected by this issue and how to address it.

5.1.15 Samba: Active Directory Domain Controller packaging changes

The Active Directory Domain Controller (AD-DC) functionality was split out of **samba**. If you are using this feature, you need to install the **samba-ad-dc** package.

5.1.16 Samba: VFS modules

The **samba-vfs-modules** package was reorganized. Most VFS modules are now included in the **samba** package. However the modules for *ceph* and *glusterfs* have been split off into **samba-vfs-ceph** and **samba-vfs-glusterfs**.

5.1.17 OpenLDAP TLS now provided by OpenSSL

The TLS support in the OpenLDAP client **libldap2** and server **slapd** is now provided by OpenSSL instead of GnuTLS. This affects the available configuration options, as well as the behavior of them.

Details about the changed options can be found in `/usr/share/doc/libldap2/NEWS.Debian.gz`.

If no TLS CA certificates are specified, the system default trust store will now be loaded automatically. If you do not want the default CAs to be used, you must configure the trusted CAs explicitly.

For more information about LDAP client configuration, see the ldap.conf.5 man page. For the LDAP server (**slapd**), see `/usr/share/doc/slapd/README.Debian.gz` and the slapd-config.5 man page.

5.1.18 bacula-director: Database schema update needs large amounts of disk space and time

The Bacula database will undergo a substantial schema change while upgrading to trixie.

Upgrading the database can take many hours or even days, depending on the size of the database and the performance of your database server.

The upgrade temporarily needs around double the currently used disk space on the database server, plus enough space to hold a backup dump of the Bacula database in `/var/cache/dbconfig-common/backups`.

Running out of disk space during the upgrade might corrupt your database and will prevent your Bacula installation from functioning correctly.

5.1.19 dpkg: warning: unable to delete old directory: ...

During the upgrade, `dpkg` will print warnings like the following, for various packages. This is due to the finalization of the `usrmerge` project, and the warnings can be safely ignored.

```
Unpacking firmware-misc-nonfree (20230625-1) over (20230515-3) ...
dpkg: warning: unable to delete old directory '/lib/firmware/wfx': Directory not empty
dpkg: warning: unable to delete old directory '/lib/firmware/ueagle-atm': Directory not␣
↪empty
```

5.1.20 Skip-upgrades are not supported

As with any other Debian release, upgrades must be performed from the previous release. Also all point release updates should be installed. See *Comenzar de un Debian «puro»*.

Skipping releases when upgrading is explicitly not supported.

For trixie, the finalization of the `usrmerge` project requires the upgrade to bookworm be completed before starting the trixie upgrade.

5.1.21 WirePlumber has a new configuration system

WirePlumber has a new configuration system. For the default configuration you don't have to do anything; for custom setups see `/usr/share/doc/wireplumber/NEWS.Debian.gz`.

5.1.22 strongSwan migration to a new charon daemon

The strongSwan IKE/IPsec suite is migrating from the legacy **charon-daemon** (using the ipsec(8) command and configured in `/etc/ipsec.conf`) to **charon-systemd** (managed with the swanctl(8) tools and configured in `/etc/swanctl/conf.d`). The trixie version of the **strongswan** metapackage will pull in the new dependencies, but existing installations are unaffected as long as **charon-daemon** is kept installed. Users are advised to migrate their installation to the new configuration following the upstream migration page ``

5.1.23 Things to do before rebooting

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 trixie.

5.2 Elementos no limitados durante el proceso de actualización

5.2.1 The directories /tmp and /var/tmp are now regularly cleaned

On new installations, *systemd-tmpfiles* will now regularly delete old files in `/tmp` and `/var/tmp` while the system is running. This change makes Debian consistent with other distributions. Because there is a small risk of data loss, it has been made «opt-in»: the upgrade to trixie will create a file /etc/tmpfiles.d/tmp.conf which reinstates the old behavior. This file can be deleted to adopt the new default, or edited to define custom rules. The rest of this section explains the new default and how to customize it.

The new default behavior is for files in `/tmp` to be automatically deleted after 10 days from the time they were last used (as well as after a reboot). Files in `/var/tmp` are deleted after 30 days (but not deleted after a reboot).

Before adopting the new default, you should either adapt any local programs that store data in `/tmp` or `/var/tmp` for long periods to use alternative locations, such as `~/tmp/`, or tell *systemd-tmpfiles* to exempt the data file from deletion by creating a file `local-tmp-files.conf` in `/etc/tmpfiles.d` containing lines such as:

```
x /var/tmp/my-precious-file.pdf
x /tmp/foo
```

Please see systemd-tmpfiles(8) and tmpfiles.d(5) for more information.

5.2.2 systemd message: System is tainted: unmerged-bin

systemd upstream, since version 256, considers systems having separate `/usr/bin` and `/usr/sbin` directories noteworthy. At startup systemd emits a message to record this fact: `System is tainted: unmerged-bin`.

It is recommended to ignore this message. Merging these directories manually is unsupported and will break future upgrades. Further details can be found in bug #1085370.

5.2.3 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.

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

Debian 13 incluye varios motores de navegador que están afectados por un flujo constante de vulnerabilidades de seguridad. La alta tasa de vulnerabilidades y la falta parcial de soporte upstream en forma de ramas de largo plazo hace muy difícil soportar estos navegadores y motores con correcciones de seguridad portadas hacia atrás. Adicionalmente, las interdependencias de bibliotecas hacen extremadamente difícil actualizar a versiones upstream más nuevas. Las aplicaciones que usan el paquete fuente **webkit2gtk** (p. ej. **epiphany**) están cubiertas por soporte de seguridad, pero las aplicaciones que usan qtwebkit (paquete fuente **qtwebkit-opensource-src**) no lo están.

Para la navegación web general se recomienda utilizar Firefox o Chromium. Se mantendrán actualizados mediante la reconstrucción de las versiones ESR actuales para stable. La misma estrategia se aplicará para Thunderbird.

Una vez que una versión se convierte en `oldstable`, los navegadores con soporte oficial pueden no continuar recibiendo actualizaciones durante el período estándar de cobertura. Por ejemplo, Chromium solo recibirá 6 meses de soporte de seguridad en `oldstable` en lugar de los típicos 12 meses.

Paquetes basados en Go y Rust

La infraestructura de Debian actualmente tiene problemas con la reconstrucción de paquetes de tipos que sistemáticamente usan enlazado estático. Con el crecimiento de los ecosistemas de Go y Rust significa que estos paquetes tendrán cobertura limitada de soporte de seguridad hasta que la infraestructura sea mejorada para manejarlos de manera sostenible.

En la mayoría de los casos si las actualizaciones están justificadas para las bibliotecas de desarrollo de Go o Rust, solo se publicarán a través de versiones menores regulares.

5.2.4 Problems with VMs on 64-bit little-endian PowerPC (ppc64el)

Currently QEMU always tries to configure PowerPC virtual machines to support 64 kiB memory pages. This does not work for KVM-accelerated virtual machines when using the default kernel package.

- If the guest OS can use a page size of 4 kiB, you should set the machine property `cap-hpt-max-page-size=4096`. For example:

```
$ kvm -machine pseries,cap-hpt-max-page-size=4096 -m 4G -hda guest.img
```

- If the guest OS requires a page size of 64 kiB, you should install the **linux-image-powerpc64le-64k** package; see *64-bit little-endian PowerPC (ppc64el) page size*.

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 *Paquetes obsoletos* para obtener una descripción).

La lista de paquetes obsoletos incluye:

- El paquete **libnss-gw-name** ha sido eliminado de trixie. El desarrollador upstream sugiere usar **libnss-myhostname** en su lugar.
- El paquete **pcregrep** ha sido eliminado de trixie. Se puede reemplazar con `grep -P` (`--perl-regexp`) o `pcre2grep` (de **pcre2-utils**).

- The **request-tracker4** package has been removed from trixie. Its replacement is **request-tracker5**, which includes instructions on how to migrate your data: you can keep the now obsolete **request-tracker4** package from bookworm installed while migrating.
- The **git-daemon-run** and **git-daemon-sysvinit** packages have been removed from trixie due to security reasons.
- The **nvidia-graphics-drivers-tesla-470** packages are no longer supported upstream and have been removed from trixie.
- The **deborphan** package has been removed from trixie. To remove unnecessary packages, `apt autoremove` should be used, after `apt-mark minimize-manual`. **debfoster** can also be a useful tool.

5.3.2 Componentes obsoletos de trixie

Con la publicación de Debian 14 (nombre en clave forky) algunas funcionalidades estarán obsoletas. Los usuarios deben migrar a otras alternativas para evitar problemas al actualizar a Debian 14.

Esto incluye las siguientes funcionalidades:

- The **sudo-ldap** package will be removed in forky. The Debian sudo team has decided to discontinue it due to maintenance difficulties and limited use. New and existing systems should use **libsss-sudo** instead.

  Upgrading Debian trixie to forky without completing this migration may result in the loss of intended privilege escalation.

  For further details, please refer to bug 1033728 and to the NEWS file in the **sudo** package.

- The **sudo_logsrvd** feature, used for sudo input/output logging, may be removed in Debian forky unless a maintainer steps forward. This component is of limited use within the Debian context, and maintaining it adds unnecessary complexity to the basic sudo package.

  For ongoing discussions, see bug 1101451 and the NEWS file in the **sudo** package.

- El paquete **libnss-docker** ya no se desarrolla upstream y requiere la versión 1.21 de la API de Docker. Esa versión de API obsoleta aún es compatible con Docker Engine v26 (incluido en Debian trixie) pero será eliminada en Docker Engine v27+ (incluido en Debian forky). A menos que se reanude el desarrollo upstream, el paquete será eliminado en Debian forky.

- Los paquetes **openssh-client** y **openssh-server** actualmente soportan autenticación e intercambio de claves GSS-API, que usualmente se usa para autenticar a servicios Kerberos. Esto ha causado algunos problemas, especialmente en el lado del servidor donde añade nueva superficie de ataque de preautenticación, y los paquetes principales de OpenSSH de Debian, por tanto dejarán de soportarlo a partir de forky.

  Si está usando autenticación GSS-API o intercambio de claves (busque opciones que empiecen con `GSSAPI` en sus archivos de configuración de OpenSSH) entonces debería instalar el paquete **openssh-client-gssapi** (en clientes) o **openssh-server-gssapi** (en servidores) ahora. En trixie, estos son paquetes vacíos que dependen de **openssh-client** y **openssh-server** respectivamente; en forky, se construirán por separado.

- sbuild-debian-developer-setup ha quedado obsoleto en favor de sbuild+unshare

  sbuild, la herramienta para construir paquetes de Debian en un entorno mínimo, ha tenido una actualización mayor y debería funcionar sin configuración adicional ahora. Como resultado, el paquete **sbuild-debian-developer-setup** ya no es necesario y ha quedado obsoleto. Puede probar la nueva versión con:

  ```
  $ sbuild --chroot-mode=unshare --dist=unstable hello
  ```

- The **fcitx** packages have been deprecated in favor of **fcitx5**

  The **fcitx** input method framework, also known as **fcitx4** or **fcitx 4.x**, is no longer maintained upstream. As a result, all related input method packages are now deprecated. The package **fcitx** and packages with names beginning with **fcitx-** will be removed in Debian forky.

Existing **fcitx** users are encouraged to switch to **fcitx5** following the fcitx upstream migration guide and Debian Wiki page.

- The **lxd** virtual machine management package is no longer being updated and users should move to **incus**.

  After Canonical Ltd changed the license used by LXD and introduced a new copyright assignment requirement, the Incus project was started as a community-maintained fork (see bug 1058592). Debian recommends that you switch from LXD to Incus. The **incus-extra** package includes tools to migrate containers and virtual machines from LXD.

- The **isc-dhcp** suite is deprecated upstream.

  If you are using **NetworkManager** or **systemd-networkd**, you can safely remove the **isc-dhcp-client** package as they both ship their own implementation. If you are using the **ifupdown** package, **dhcpcd-base** provides a replacement. The ISC recommends the **Kea** package as a replacement for DHCP servers.

5.4 Bugs graves conocidos

Aunque Debian publica versiones cuando están listas, eso desafortunadamente no significa que no haya bugs conocidos. Como parte del proceso de publicación todos los bugs de severidad grave o superior son rastreados activamente por el Release Team, así que un resumen de esos bugs que fueron etiquetados para ser ignorados en la última parte de la publicación de trixie se puede encontrar en el Debian Bug Tracking System. Los siguientes bugs estaban afectando a trixie al momento de la publicación y vale la pena mencionarlos en este documento:

Número de bug	Paquete (fuente o binario)	Descripción
1032240	**akonadi-backend-mysql**	el servidor akonadi falla al iniciar ya que no puede conectarse a la base de datos mysql
1102690	**flash-kernel**	available kernels not always updated in u-boot configuration

CAPÍTULO 6

Más información sobre Debian

6.1 Para leer más

Además de estas notas de publicaciones y la guía de instalación (en https://www.debian.org/releases/trixie/installmanual), hay más documentación de Debian disponible a través del Proyecto de Documentación de Debian (DDP). El objetivo de este proyecto es crear y mantener documentación de alta calidad para los usuarios y desarrolladores de Debian. En este proyecto encontrará documentos como la Guía de Referencia, la Guía del Nuevo Desarrollador, las PUF de Debian y muchos más documentos. Encontrará todos los detalles de los recursos disponibles en la web de Documentación de Debian y en el Wiki de Debian.

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

La lista de correo que más interesará a los usuarios de Debian es la lista debian-usr (en inglés) y las otras listas debian-user-idioma (para otros idiomas). Por ejemplo, puede utilizar la lista debian-user-spanish para hacer consultas o preguntas en español. Puede encontrar más información de las listas, incluyendo los detalles y cómo suscribirse en https://lists.debian.org/. Por favor, consulte los archivos de la lista para buscar respuestas a sus preguntas antes de hacer una pregunta nueva y adhiérase al comportamiento y etiqueta estándar utilizados en listas de correo.

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.

For more information on OFTC please visit the website.

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.

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 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 de desarrollo. Para mantener la distribución de alta calidad de Debian puede informar sobre fallos 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 o a traducir 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 (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 de Debian, como pueden ser la adaptación a alguna arquitectura concreta, y Debian Pure Blends 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

Gestión de su sistema bookworm antes de la actualización

Este apéndice contiene la información sobre cómo asegurarse de que puede instalar o actualizar los paquetes de bookworm antes de actualizar a trixie.

7.1 Actualizar su sistema bookworm

Básicamente esto no es diferente de cualquier otra actualización de bookworm que haya estado haciendo. La única diferencia es que primero necesita asegurarse de que su lista de paquetes aún contenga referencias a bookworm como se explica en *Checking your APT source-list files*.

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

7.2 Checking your APT configuration

If any of the lines in your APT sources files (see sources.list(5)) contain references to «stable», this is effectively pointing to trixie already. This might not be what you want if you are not yet ready for the upgrade. If you have already run `apt update`, you can still get back without problems by following the procedure below.

Si también ha instalado los paquetes desde trixie, probablemente ya no tiene mucho sentido instalar paquetes desde bookworm. 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.

As root, open the relevant APT sources file(s) (such as `/etc/apt/sources.list` or any file under `/etc/apt/sources.list.d/`) with your favorite editor, and check all lines beginning with

- `deb http:`
- `deb https:`
- `deb tor+http:`
- `deb tor+https:`
- `URIs: http:`

- `URIs: https:`
- `URIs: tor+http:`
- `URIs: tor+https:`

para ver si existe alguna referencia a «stable». Si encuentra alguna, cambie «stable» por «bookworm».

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 bookworm o de trixie.

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.

7.3 Realizando la actualización a la última versión de bookworm

Para actualizar todos los paquetes al estado de la última versión menor de bookworm, haga

```
# apt full-upgrade
```

7.4 Borrar ficheros de configuración obsoletos

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

CAPÍTULO 8

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. Barrat (varios arreglos desde 2013),
- Adam Di Carlo (versiones anteriores),
- Andreas Barth aba (versiones anteriores: 2005 - 2007),
- Andrei Popescu (diversas contribuciones),
- Anne Bezemer (versión anterior),
- Bob Hilliard (versión anterior),
- Charles Plessy (descripción del problema GM965),
- Christian Perrier bubulle (Instalación de Lenny),
- Christoph Berg (Problemas específicos de PostgreSQL),
- Daniel Baumann (Debian Live),
- David Prévot taffit (versión Wheezy),
- Eddy Petrișor (diversas contribuciones),
- Emmanuel Kasper (backports),
- Esko Arajärvi (reescritura de la actualización de X11),
- Frans Pop fjp (versión anterior Etch),
- Giovanni Rapagnani (innumerables contribuciones),
- Gordon Farquharson (problemas de la adaptación a ARM),
- Hideki Yamane henrich (contribuyendo desde 2006),
- Holger Wansing holgerw (contribuyendo desde 2009),
- Javier Fernández-Sanguino Peña jfs (versión Etch, versión Squeeze),
- Jens Seidel (traducción al alemán y numerosas contribuciones),

- Jonas Meurer (problemas del syslog),
- Jonathan Nieder (versión Squeeze, versión Wheezy),
- Joost van Baal-Ilić joostvb (versión Wheezy, versión Jessie),
- Josip Rodin (versiones anteriores),
- Julien Cristau jcristau (versión Squeeze, versión Wheezy),
- Justin B Rye (Arreglos a la versión en inglés),
- LaMont Jones (descripción de problemas de NFS),
- Luk Claes (gestor de la motivación de los editores),
- Martin Michlmayr (problemas de la adaptación a ARM),
- Michael Biebl (problemas del syslog),
- Moritz Mühlenhoff (diversas contribuciones),
- Niels Thykier nthykier (versión Jessie),
- Noah Meyerhans (innumerables contribuciones),
- Noritada Kobayashi (traducción al japonés (coordinación) y numerosas contribuciones),
- Osamu Aoki (diversas contribuciones),
- Paul Gevers elbrus (versión Buster),
- Peter Green (notas de la versión del núcleo),
- Rob Bradford (versión Etch),
- Samuel Thibault (descripción del soporte de Braille en d-i),
- Simon Bienlein (descripción del soporte de Braille en d-i),
- Simon Paillard spaillar-guest (innumerables contribuciones),
- Stefan Fritsch (descripción de los problemas de Apache),
- Steve Langasek (versión Etch),
- Steve McIntyre (Debian CDs),
- Tobias Scherer (descripción de "proposed-update"),
- victory victory-guest (arreglos de marcado, contribuyendo desde 2006),
- Vincent McIntyre (descripción de "proposed-update"),
- W. Martin Borgert (edición de la versión de Lenny, cambio a DocBook XML).

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, Fernando González de la Requena y Wilmer Narváez.