Notas de publicación de Debian 10 (buster), IBM System z

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

4 de julio de 2022

Esta documentación es software libre; puede redistribuirla o modificarla bajo los términos de la Licencia Pública General GNU, versión 2, publicada por la «Free Software Foundation».

Este programa se distribuye con el deseo de ser útil, pero SIN GARANTÍA ALGUNA; ni siquiera la garantía implícita de MERCADEO o AJUSTE A PROPÓSITOS ESPECÍFICOS. Si desea más detalles, consulte la Licencia Pública General de GNU.

Debería haber recibido una copia de la Licencia Pública General de GNU junto con este programa; si no fue así, escriba a la Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

El texto de la licencia se puede encontrar también en https://www.gnu.org/licenses/gpl-2.0.html y en /usr/share/common-licenses/GPL-2 en los sistemas Debian.

Índice general

1. Introducción **1**
1.1. Cómo informar de fallos en este documento . . . 1
1.2. Cómo contribuir con informes de actualización . . . 1
1.3. Fuentes de este documento . . . 2

2. Las novedades de Debian 10 **3**
2.1. Arquitecturas soportadas . . . 3
2.2. ¿Qué novedades hay en la distribución? . . . 3
2.2.1. Arranque seguro UEFI . . . 4
2.2.2. AppArmor activo por omisión . . . 4
2.2.3. Bastionado opcional de APT . . . 5
2.2.4. Actualizaciones desatendidas para publicaciones estables . . . 5
2.2.5. Mejora sustancial en las páginas de manual para usuarios que hablan alemán . . . 5
2.2.6. Filtrado de red basado en nftables por omisión . . . 5
2.2.7. Cryptsetup utiliza el formato de LUKS2 en disco . . . 6
2.2.8. Impresión sin controladores en CUPS 2.2.10 . . . 6
2.2.9. Soporte básico de dispositivos basados en Allwinner A64 . . . 7
2.2.10. Noticias de la mezcla Debian Med . . . 7
2.2.11. GNOME utiliza Wayland por omisión . . . 7
2.2.12. Fusión de /usr en nuevas instalaciones . . . 7
2.2.13. Noticias del grupo Debian Live . . . 8

3. Sistema de instalación **9**
3.1. Novedades del sistema de instalación . . . 9
3.1.1. Instalación automatizada . . . 9

4. Actualizaciones desde Debian 9 (stretch) **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 . . . 11
4.1.3. Prepararse para la indisponibilidad de servicios . . . 12
4.1.4. Prepararse para la recuperación . . . 12
4.1.4.1. Intérprete de línea de órdenes de depuración durante el arranque con initrd 12
4.1.4.2. Intérprete de línea de órdenes de depuración durante el arranque con systemd . . . 13
4.1.5. Preparar un entorno seguro para la actualización . . . 13
4.1.6. Verificar el soporte de los nombres de interfaces de red . . . 13
4.2. Verificar el estado de configuración de APT . . . 13
4.2.1. La sección “proposed-updates” . . . 14
4.2.2. Fuentes no oficiales . . . 14
4.2.3. Desactivar el bloqueo de APT . . . 14
4.2.4. Verificar el estado de los paquetes . . . 14
4.3. Preparar las fuentes de orígenes para APT . . . 15
4.3.1. Añadir fuentes en Internet para APT . . . 16
4.3.2. Añadir las réplicas locales para APT . . . 16
4.3.3. Añadir fuentes para APT de medios ópticos . . . 17
4.4. Actualizar los paquetes . . . 17
4.4.1. Grabar la sesión . . . 17
4.4.2. Actualizar las listas de paquetes . . . 18
4.4.3. Asegúrese de que tiene suficiente espacio libre para actualizar . . . 18
4.4.4. Actualización mínima del sistema . . . 20
4.4.5. Actualizar el sistema . . . 21
4.5. Posibles problemas durante o después de la actualización . . . 21
4.5.1. Dist-upgrade falla con «No se pudo realizar la configuración inmediata» . . . 21

4.5.2. Eliminaciones esperadas . . . 21
4.5.3. Bucles en Conflictos o Pre-Dependencias . . . 22
4.5.4. Conflictos de archivo . . . 22
4.5.5. Cambios de configuración . . . 22
4.5.6. Cambio de la sesión en consola . . . 23
4.6. Actualización de su núcleo y paquetes relacionados . . . 23
4.6.1. Instalación de un metapaquete del núcleo . . . 23
4.7. Prepararse para la siguiente distribución . . . 24
4.7.1. Purgando los paquetes eliminados . . . 24
4.8. Paquetes obsoletos . . . 24
4.8.1. Paquetes «dummy» de transición . . . 25

5. Problemas que debe tener en cuenta para buster **27**
5.1. Actualizar elementos específicos para buster . . . 27
5.1.1. s390x ISA incrementado a z196 . . . 27
5.1.2. Opción de montaje hidepid de procfs no soportada . . . 27
5.1.3. ypbind no puede iniciarse con -no-dbus . . . 27
5.1.4. NIS server does not answer NIS client requests by default . . . 27
5.1.5. sshd falla al autenticar . . . 28
5.1.6. Los demonios no arrancan o el sistema parece colgarse durante el arranque . . . 28
5.1.7. Migración de los nombres de interfaz de red antiguos . . . 28
5.1.8. Configuración de módulos para interfaces agrupados y «dummy» . . . 29
5.1.9. Versión por omisión de OpenSSL e incremento del nivel de seguridad . . . 29
5.1.10. Algunas aplicaciones no funcionan con GNOME en Wayland . . . 30
5.1.11. Paquetes obsoletos notables . . . 30
5.1.12. Componentes obsoletos de buster . . . 30
5.1.13. Cosas a hacer después de la actualización y antes de reiniciar . . . 31
5.1.14. Los paquetes relacionados con SysV init ya no son necsearios . . . 31
5.2. Limitaciones en el soporte de seguridad . . . 31
5.2.1. Estado de seguridad en los navegadores web y sus motores de render . . . 31
5.2.2. Paquetes basados en Go . . . 32
5.3. Problemas específicos de paquetes . . . 32
5.3.1. Cambio en las semánticas del uso de variables de entorno para su . . . 32
5.3.2. Reindexación necesaria en bases de datos PostgreSQL existentes . . . 32
5.3.3. mutt y neomutt . . . 32
5.3.4. Acceso de la configuración de GNOME sin ratón . . . 33
5.3.5. gnome-disk-utility fails to change LUKS password causing permanent data loss (buster 10.0 only) . . . 33
5.3.6. evolution-ews se ha eliminado, y se eliminarán los buzones de correo que utilicen Exchange, Office365 o un servidor de Outlook . . . 33
5.3.7. El instalador Calamares deja claves de cifrado de disco legibles . . . 33
5.3.8. S3QL URL changes for Amazon S3 buckets . . . 33
5.3.9. Split in configuration for logrotate . . . 33
5.3.10. The `rescue` boot option is unusable without a root password . . . 34

6. Más información sobre Debian **35**
6.1. Para leer más . . . 35
6.2. Cómo conseguir ayuda . . . 35
6.2.1. Listas de correo electrónico . . . 35
6.2.2. Internet Relay Chat (IRC) . . . 35
6.3. Cómo informar de fallos . . . 35
6.4. Cómo colaborar con Debian . . . 36

7. Glosario **37**

A. Gestión de su sistema stretch antes de la actualización **39**
A.1. Actualizar su sistema stretch 39
A.2. Comprobar su lista de fuentes APT 39
A.3. Borrar ficheros de configuración obsoletos 40
A.4. Actualización de localizaciones antiguas a UTF-8 40

B. Personas que han contribuido a estas notas de publicación **41**

Índice alfabético **43**

Capítulo 1

Introducción

Este documento informa a los usuarios de la distribución Debian sobre los cambios más importantes de la versión 10 (nombre en clave «buster»).

Las notas de publicación proporcionan la información sobre cómo actualizar de una forma segura desde la versión 9 (nombre en clave «stretch») 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/buster/releasenotes`. Si tiene alguna duda, compruebe la fecha en la primera página para asegurarse que está Vd. leyendo la última versión.

ATENCIÓN

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

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

1.1. Cómo informar de fallos en este documento

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

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

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

1.2. Cómo contribuir con informes de actualización

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

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

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

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

NOTA

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

1.3. Fuentes de este documento

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

Capítulo 2

Las novedades de Debian 10

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

2.1. Arquitecturas soportadas

Las siguientes son las arquitecturas oficialmente soportadas en Debian 10:

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

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

2.2. ¿Qué novedades hay en la distribución?

Esta nueva versión de Debian trae de nuevo muchos más programas que su predecesora stretch; la distribución incluye más de 13370 paquetes nuevos, para un total de más de 57703 paquetes. La mayor parte de los programas que se distribuyen se han actualizado: más de 35532 paquetes de programas (corresponde a un 62 % de los paquetes en stretch). También se han eliminado por varios motivos un número significativo de paquetes (más de 7278, 13 % de los paquetes en stretch). No verá ninguna actualización para estos paquetes y se marcarán como «obsoletos» en los programas de gestión de paquetes. Consulte la sección Sección 4.8.

Debian trae de nuevo varias aplicaciones de escritorio y entornos. Entre otros ahora incluye los entornos de escritorio GNOME 3.30, KDE Plasma 5.14, LXDE 10, LXQt 0.14, MATE 1.20 y Xfce 4.12.

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

- LibreOffice se ha actualizado a la versión 6.1;
- Calligra se ha actualizado a la versión 3.1.
- GNUcash se ha actualizado a la versión 33.4;

Con buster, Debian introduce por primera vez un sistema de control de acceso obligatorio por omisión. Las nuevas instalaciones de Debian buster tendrán AppArmor instalado por omisión. Consulte más abajo para más información.

Además, buster es la primera publicación de Debian que se distribuye con programas basados en Rust como Firefox, ripgrep, fd, exa, etc. y un número significativo de librerías basadas en Rust (más de 450). Buster se publica con Rustc 1.34.

Las actualizaciones de otras aplicaciones de escritorio incluyen la actualización a Evolution 3.30.

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

Paquete	**Versión en 9 (stretch)**	**Versión en 10 (buster)**
Apache	2.4.25	2.4.38
BIND Servidor DNS	9.10	9.11
Cryptsetup	1.7	2.1
Dovecot MTA	2.2.27	2.3.4
Emacs	24.5 y 25.1	26.1
Exim servidor de correo predeterminado	4.89	4.92
La colección de compilador GNU como el compilador por omisión	6.3	7.4 y 8.3
GIMP	2.8.18	2.10.8
GnuPG	2.1	2.2
Inkscape	0.92.1	0.92.4
La biblioteca de C de GNU	2.24	2.28
lighttpd	1.4.45	1.4.53
imagen del núcleo de Linux	serie 4.9	serie 4.19
LLVM/Clang toolchain	3.7	6.0.1 y 7.0.1 (por omisión)
MariaDB	10.1	10.3
Nginx	1.10	1.14
OpenJDK	8	11
OpenSSH	7.4p1	7.9p1
Perl	5.24	5.28
PHP	7.0	7.3
Postfix MTA	3.1.8	3.3.2
PostgreSQL	9.6	11
Python 3	3.5.3	3.7.3
Rustc		1.34
Samba	4.5	4.9
Vim	8.0	8.1

2.2.1. Arranque seguro UEFI

El arranque seguro («Secure Boot», N. del T.) es una funcionalidad activa en la mayoría de los PCs que previene la carga de código sin firmar, protegiéndolos frente a unos tipos de virus de arranque y «rookits».

Debian puede instalarse ahora en la mayoría de los PCs que tienen el arranque seguro habilitado.

Es posible activar el arranque seguro en un sistema que ya tiene una instalación de Debian, si ya arranca con UEFI. Antes de hacerlo, es necesario instalar `shim-signed`, `grub-efi-amd64-signed` o `grub-efi-ia32-signed`, y un paquete del núcleo de Linux de buster.

Algunas funcionalidades de GRUB y de Linux están restringidas en el modo de arranque seguro para evitar modificaciones de su código.

Puede encontrar más información en el wiki de Debian en la página SecureBoot (`https://wiki.debian.org/SecureBoot`).

2.2.2. AppArmor activo por omisión

En Debian buster `AppArmor` está activado por omisión. `AppArmor` es un sistema de control de acceso obligatorio que permite restringir las capacidades de un programa (como puedan ser los permisos de

lectura, escritura y ejecución sobre archivos o los permisos sobre montaje, ptrace y señales) a través de una serie de perfiles definidos por programa.

El paquete `apparmor` se distribuye con perfiles de AppArmor para distintos programas. Algunos otros paquetes, como por ejemplo `evince`, incluyen perfiles para los programas que incluyen. Puede encontrar más perfiles en el paquete `apparmor-profiles-extra`.

`AppArmor` se instala a través de las `Recommendaciones` del paquete del núcleo Linux de buster. Puede instalar el paquete `apparmor` manualmente para activar `AppArmor` en los sistemas que están configurados para no instalar paquetes recomendados por omisión.

2.2.3. Bastionado opcional de APT

Todos los métodos que ofrece APT (p.ej. http, y https) exceptuando los métodos cdrom, gpgv, y rsh pueden utilizar «seccomp-BPF sandboxing» tal y como lo ofrece el núcleo de Linux. Esta función restringe la lista de llamadas del sistema permitdas, y atrapa otras con una señal `SIGSYS`. Esta ejecución registringida es actualmente opcional y tiene que activarse con:

```
APT::Sandbox::Seccomp es un valor booleano para activarlo/desactivarlo
```

Puede utilizar dos opciones para configurar esta funcionalidad:

```
APT::Sandbox::Seccomp::Trap es la lista de nombres de más llamadas al ↩
    sistema a capturar
APT::Sandbox::Seccomp::Allow es la lista de nombres de llamadas al sistema ↩
    a permitir
```

2.2.4. Actualizaciones desatendidas para publicaciones estables

Las versiones anteriores de `unattended-upgrades` estaban configuradas por omisión para instalar sólo actualizaciones del grupo de seguridad. En buster también permite actualizar automáticamente de la última publicación estable. Consulte el archivo NEWS.Debian para más información.

2.2.5. Mejora sustancial en las páginas de manual para usuarios que hablan alemán

Se ha extendido substancialmente la documentación (`man`-pages) para varios proyectos como `systemd`, `util-linux` y `mutt`. Si desea beneficiarse de estas mejoras debe instalar el paquete `manpages-de`. Se proporcionarán nuevas/mejoradas traducciones durante el ciclo de vida de buster a través del archivo `backports`.

2.2.6. Filtrado de red basado en nftables por omisión

A partir de la versión 1.8.2 del paquete binario `iptables` se incluyen `iptables-nft` y `iptables-legacy`, dos variantes del interfaz de línea de órdenes de `iptables`. La variante nftables, que utiliza el subsistema del núcleo `nf_tables` es utilizada por omisión en buster. La variante antigua utiliza el subsistema del núcleo de Linux `x_tables`. Se puede utilizar el sistema `update-alternatives` para seleccionar una variante o la otra.

Esto aplica a todas las herramientas y utilidades relacionadas:

- iptables
- iptables-save
- iptables-restore
- ip6tables
- ip6tables-save
- ip6tables-restore

- arptables
- arptables-save
- arptables-restore
- ebtables
- ebtables-save
- ebtables-restore

Para todas estas hay ahora una variante `-nft` y `-legacy`. La opción `-nft` option es para los usuarios que no pueden o no quieren migrar a la interfaz de línea de órdenes `nftables` nativa. Sin embargo, se recomienda encarecidamente a los usuarios que cambien a la interfaz `nftables` en lugar de utilizar `iptables`.

`nftables` ofrece un reemplazo completo de `iptables`, con mejor rendimiento, sintaxis refrescada, mejor soporte de cortafuegos con pila dual IPv4/IPv6, operaciones atómicas para actualizaciones dinámicas de las reglas, una API para aplicaciones, clasificación de paquetes más rápida a través de mejoras de la infrastructura de mapas y de conjuntos genéricos, y muchas otras mejoras (`https://wiki.nftables.org`).

Este cambio está en línea con los cambios introducidos por otras distribuciones importantes de Linux, como Red Hat, que ahora utiliza `nftables` como su herramienta de cortafuegos por omisión (`https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8-beta/html-single/8.0_beta_release_notes/index#networking_2`).

Tenga en cuenta también que todos los binarios de `iptables` se instalan en `/usr/sbin` en lugar de en `/sbin`. Existe un enlace simbólico por compatibilidad, pero se eliminará después del ciclo de publicación de buster. Los programas que incluyan la ruta completa a los binarios deben corregirse y debe evitarse ese tipo de configuración.

Tiene disponible documentación extensiva en los archivos README y NEWS en el Wiki de Debian (`https://wiki.debian.org/nftables`).

2.2.7. Cryptsetup utiliza el formato de LUKS2 en disco

La versión de `cryptsetup` que se distribuye con Debian buster utiliza el nuevo formato `LUKS2` en disco. Los nuevos volúmenes `LUKS` utilizarán este formato por omisión.

A diferencia del formato anterior `LUKS1`, `LUKS2` proporciona redundancia de metadatos, detección de corrupción de metadatos y algoritmos `PBKDF`. También incluye soporte de cifrado autenticado, pero éste está marcado aún como experimental.

Los volúmenes `LUKS1` existentes no se actualizarán automáticamente. Pueden convertirse al nuevo formato, pero no estarán disponibles todas las funcionalidades de `LUKS2` debido a incompatibilidades en los tamaños de la cabecera. Consulte la página de manual de cryptsetup (`https://manpages.debian.org/buster/cryptsetup`) para más información.

Tenga en cuenta que el cargador de arranque GNU GRUB aún no ofrece soporte del formato `LUKS2`. Consulte la documentación (`https://cryptsetup-team.pages.debian.net/cryptsetup/encrypted-boot.html`) correspondiente para más información sobre cómo instalar Debian 10 con el arranque cifrado.

2.2.8. Impresión sin controladores en CUPS 2.2.10

Debian 10 ofrece CUPS 2.2.10 y `cups-filters` versión 1.21.6. Los dos juntos le ofrecen a un usuario todo lo que necesita para beneficiarse de la impresión sin controladores (`https://wiki.debian.org/DriverlessPrinting`). El requisito principal es que exista una cola de impresión de red o una impresora que ofrezca el servicio «Airprint». Es muy probable que una impresora moderna IPP tenga la funcionalidad de «AirPrint», en Debian CUPS se dispone siempre de una cola de impresión capaz de utilizar esta funcionalidad.

Esencialmente, las publicaciones en la red a través del servicio DNS-SD (Bonjour) de un servidor CUPS que ofrezca una cola de impresión, o de aquellas impresoras IPP que lo hagan, se mostrarán en los diálogos de impresión de las aplicaciones sin que sea necesaria ninguna acción por parte del usuario. Un beneficio adicional es que ya no es necesario utilizar controladores de impresión de los fabricantes no libres o de complementos adicionales para imprimir en este tipo de impresoras.

Una instalación por omisión del paquete `cups` también instala el paquete `cups-browsed`. Las colas de impresión y las impresoras IPP se configurarán y gestionarán de forma automática con esta utilidad. Esta la forma recomendada (`https://wiki.debian.org/QuickPrintQueuesCUPS`) para un usuario para ofrece una experiencia de impresión sin controladores transparente y sin problemas.

2.2.9. Soporte básico de dispositivos basados en Allwinner A64

Gracias a los esfuerzos de la comunidad linux-sunxi (`https://linux-sunxi.org`), Debian buster tendrá soporte básico de muchos dispositivos que están basados en el Allwinner A64 SoC. Esto incluye dispositivos como: FriendlyARM NanoPi A64; Olimex A64-OLinuXino y TERES-A64; PINE64 PINE A64/A64/A64-LTS, SOPINE, y Pinebook; SINOVOIP Banana Pi BPI-M64; y Xunlong Orange Pi Win(Plus).

Las funciones esenciales de estos dispositivos (p.ej. consola serie, red ethernet, puertos USB y salida de vídeo básica) deberían funcionar con el núcleo de buster. Algunas funcionalidades más avanzadas (p.ej. audio o vídeo acelerado) están incluídas o se espera incuirlas en núcleos posteriores, que se ofrecerán de la forma habitual a través del archivo backports (`https://backports.debian.org`). Consulte la página de estado (`https://linux-sunxi.org/Linux_mainlining_effort`) para conocer más detalles de esta iniciativa.

2.2.10. Noticias de la mezcla Debian Med

El equipo de Debian Med ha añadido algunos paquetes nuevos y actualizaciones a los paquetes dirigidos a las ciencias de la vida y a la medicina. Se continua realizando un esfuerzo para dar soporte para la integración continua de paquetes en estos campos.

Para instalar paquetes mantenidos por el grupo Debian Med, instale los paquetes que comienzan por `med-*`, que están en la versión 3.3 para Debian buster. Puede consultar en las páginas de las tareas de Debian Med (`http://blends.debian.org/med/tasks`) la amplia variedad de programas biológicos y médicos disponible en Debian.

2.2.11. GNOME utiliza Wayland por omisión

Igual que lo hace el desarrollo principal, GNOME en buster utiliza el servidor de visualización Wayland en lugar de Xorg. Wayland tiene un diseño más sencillo y más moderno, lo que tiene ciertas ventajas desde el punto de vista de la seguridad.

El servidor de visualización Xorg se sigue instalando por omisión y el gestor de pantalla por omisión le permite elegirlo como servidor de visualización para la siguiente sesión, lo cual puede ser necesario si quiere utilizar algunas aplicaciones (consulte Sección 5.1.10).

Se recomienda a aquellas personas que requieran las funcionalidades para accesibilidad del servidor de visualización, p.ej. los atajos globales de teclado, que utilicen Xorg en lugar de Wayland.

2.2.12. Fusión de /usr en nuevas instalaciones

En las nuevas instalaciones, los contenidos de `/bin`, `/sbin` y `/lib` se instalarán en sus respectivas ubicaciones en `/usr` por omisión. Se creará un enlace `/bin`, `/sbin` y `/lib` apuntándolas hacia sus directorios equivalentes bajo `/usr/`. De forma gráfica:

```
/bin → /usr/bin
/sbin → /usr/sbin
/lib → /usr/lib
```

Los sistemas se quedan como están cuando se actualizan a buster, aunque se puede utilizar el paquete `usrmerge` para hacer la conversión si se desea. El proyecto freedesktop.org (`https://www.freedesktop.org`) proporciona un Wiki (`https://www.freedesktop.org/wiki/Software/systemd/TheCaseForTheUsrMerge/`) que describe la mayoría de las razones.

Este cambio no debería impactar a los usuarios normales que sólo ejecutan paquetes que provienen de Debian, pero es algo que tienen que tener presente los usuarios que utilizan o construyen paquetes o programas de terceros.

2.2.13. Noticias del grupo Debian Live

El equipo de Debian Live se enorgullece de introducir las ISOs «live» de LXQt como una nueva variante. LXQt es un entorno de escritorio de QT ligero. No se introducirá en su camino. No se colgará o ralentizará su sistema. Su foco es proporcionar un entorno de escritorio clásico con una apariencia moderna.

El entorno de escritorio LXQt ofrecido por el proyecto Debian Live es una versión pura y sin modificaciones. Se ofrece la experiencia de entorno de escritorio estándar que los desarrolladores de LXQt crearon para este sistema operativo popular. Los usuarios que lo utilizan pueden experimentar la organización estándar de LXQt que está formado por un único panel (barra de tareas) que se encuentra en la parte inferior de la pantalla. Este panel incluye componentes básicos como el Menú Principal, el gestor de tareas, el lanzador de aplicaciones, el área de notificaciones del sistema y el calendario integrado.

Las imágenes «live» de buster proporcionan funcionalidades que otras distribuciones han adoptado, como es el instalador Calamares. Calamares es un proyecto de instalador independiente (lo llaman la "plataforma de instalador universal") que ofrece un interfaz basado en Qt para instalar el sistema. No reemplaza al programa debian-installer en las imágenes «live». En realidad sirve a una audiencia distinta.

Calamares es muy fácil de utilizar, con un sistema de particionado guiado amistoso y una configuración muy sencilla para establecer discos cifrados. No cobre todas las funcionalidades avanzadas del instalador de Debian debian-installer (aunque recientemente incorporó soporte de RAID) y no ofrece tampoco un modo de instalación desatendido. Sin embargo, el interfaz de Calamares es mucho más sencillo para instalar un sistema para el 95 %+ de los usuarios de entornos de escritorio y portátiles. Calamares es una forma mucho más fácil para instalar un sistema, lo que le hace apropiado para los sistemas «live». El programa «debian-installer» sigue estando disponible tanto en versión GUI como de interfaz de texto, para aquellos que necesitan un sistema de instalación más complicado, o que están haciendo instalaciones masivas.

Debian Live Buster vuelve a introducir la imagen «live» estándar. Esta es una imagen básica de Debian que contiene un sistema de Debian base sin ningún interfaz de usuario gráfico. El tiempo de instalación es mucho más rápido que si se utiliza una imagen de instalación mínima de Debian. Esto se debe a que se instala desde una imagen squashfs en lugar de instalar los archivos del sistema utilizando **dpkg**.

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 buster junto con la «Guía de instalación» en la página web de Debian (`https://www.debian.org/releases/buster/debian-installer/`).

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

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

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

3.1. Novedades del sistema de instalación

Se ha realizado mucho desarrollo en el instalador de Debian desde su primera versión oficial en Debian 9, dando como resultado una mejora en el soporte de hardware y algunas funcionalidades nuevas muy interesantes.

Una de las mejoras notables es el soporte inicial a «UEFI Secure Boot» (consulte Sección 2.2.1) que se ha introducido en las imágenes de instalación.

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

3.1.1. Instalación automatizada

Algunos de los cambios mencionados en la sección anterior también implican cambios en la automatización del instalador utilizando archivos de preconfiguración. Esto significa que si tiene archivos de preconfiguración que funcionaban con el instalador de stretch no se puede asegurar que funcionen con el nuevo instalador sin que se modifiquen.

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

Capítulo 4

Actualizaciones desde Debian 9 (stretch)

4.1. Prepararse para la actualización

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

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

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

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

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

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

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

4.1.2. Informar a los usuarios anticipadamente

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

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

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

4.1.3. Prepararse para la indisponibilidad de servicios

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

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

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

4.1.4. Prepararse para la recuperación

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

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

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

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

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

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

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

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

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

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

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

de dispositivos se han asignado a qué discos, debería comparar esa información con la salida de `echo $ROOT` para asegurarse que el sistema de archivos está en el dispositivo que esperaba.

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

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

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

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

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

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

4.1.5. Preparar un entorno seguro para la actualización

IMPORTANTE

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

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

4.1.6. Verificar el soporte de los nombres de interfaces de red

Existe el riesgo de perder la conectividad a la red al migrar a buster en aquellos sistemas que se actualicen de publicaciones anteriores que aún utilicen los nombres de interfaces de red como `eth0` o `wlan0`. Puede consultar las instrucciones de migración en Sección 5.1.7.

4.2. Verificar el estado de configuración de APT

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

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

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

```
$ aptitude search '~i(!~ODebian)'
$ apt-forktracer | sort
```

No se da soporte a actualizaciones de versiones de Debian anteriores a 9 (stretch). Por favor, siga las instrucciones en las Notas de publicación para Debian 9 (`https://www.debian.org/releases/stretch/releasenotes`) para actualizarse primero a Debian 9.

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

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

Es una buena idea eliminar paquetes obsoletos de su sistema antes de actualizar.

4.2.1. La sección "proposed-updates"

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

4.2.2. Fuentes no oficiales

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

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

4.2.3. Desactivar el bloqueo de APT

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

4.2.4. 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
```

[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.

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

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

o

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

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

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

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

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

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

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

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

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

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

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

4.3. Preparar las fuentes de orígenes para APT

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

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

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

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

4.3.1. Añadir fuentes en Internet para APT

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

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

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

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

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

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

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

```
      http://mirrors.kernel.org/debian/dists/buster/main/binary-s390x/...
      http://mirrors.kernel.org/debian/dists/buster/contrib/binary-s390x/...
```

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

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

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

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

4.3.2. Añadir las réplicas locales para APT

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

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

```
      /var/local/debian/dists/buster/main/binary-s390x/...
      /var/local/debian/dists/buster/contrib/binary-s390x/...
```

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

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

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

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

4.3.3. Añadir fuentes para APT de medios ópticos

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

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

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

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

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

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

Después, ejecute:

```
# apt-cdrom add
```

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

4.4. Actualizar los paquetes

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

NOTA

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

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

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

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

NOTA

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

4.4.1. Grabar la sesión

Se recomienda encarecidamente que utilice el programa **/usr/bin/script** para guardar una transcripción de la sesión de actualización. Así, si ocurre algún problema, tendrá un registro de lo que ha

sucedido y, si fuera necesario, podrá proporcionar la información detallada cuando envíe un informe de fallo. Para iniciar la transcripción, teclee:

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

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

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

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

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

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

```
# scriptreplay ~/upgrade-busterstep.time ~/upgrade-busterstep.script
```

4.4.2. Actualizar las listas de paquetes

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

```
# apt update
```

NOTA

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

4.4.3. Asegúrese de que tiene suficiente espacio libre para actualizar

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

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

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

NOTA

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

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

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

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

- Elimine aquellos paquetes que se han descargado previamente para su instalación (en `/var/cache/apt/archive`). Puede utilizar la orden **apt clean** para borrar todos los archivos de paquetes previamente descargados.

- Eliminar paquetes olvidados. Si ha utilizado **aptitude** o **apt** para instalar manualmente paquetes de stretch, la herramienta hará un seguimiento de los paquetes que haya instalado y podrá marcar como redundantes aquellos paquetes que se obtuvieron solo para cumplir las dependencias pero que ya no se necesitan porque el paquete que los necesitaba se ha eliminado. No se marcarán como obsoletos aquellos paquetes que haya instalado manualmente. Pero si lo hará para aquellos paquetes que se instalaron automáticamente para cumplir dependencias. Para eliminar automáticamente los paquetes instalados que no se necesitan puede ejecutar lo siguiente:

  ```
  # apt-get autoremove
  ```

  También puede utilizar para encontrar paquetes redundantes **deborphan**, **debfoster** o **cruft**. No elimine a ciegas los paquetes que le indiquen estas herramientas, especialmente si utiliza opciones agresivas, distintas a las definidas por omisión, que pueden dar lugar a muchos falsos positivos. Se le recomienda encarecidamente que revise los paquetes que éstas le sugieren eliminar (esto es: sus contenidos, su tamaño y descripción) antes de eliminarlos

- Elimine paquetes que consumen mucho espacio y que no necesita actualmente (siempre puede instalarlos después de la actualización). Puede utilizar la orden **popcon-largest-unused** para listar los paquetes que no utiliza que consumen más espacio si tiene instalado `popularity-contest`. Puede encontrar los paquetes que consumen más espacio con **dpigs** (disponible en el paquete `debian-goodies`) o con **wajig** (ejecutando `wajig size`). También puede encontrarlos con `aptitude`. Ejecute **aptitude** en el modo de terminal completo, seleccione Vistas y Nueva vista de paquetes plana, pulse la tecla **l** e introduzca `~i`, a continuación pulse la tecla **S** e introduzca `~installsize`. Una vez hecho esto, dispondrá de una lista de paquetes sobre la que puede trabajar.

- Puede eliminar las traducciones y los archivos de localización del sistema si no los necesita. Para ello puede instalar el paquete `localepurge`, configurándolo para que solo se mantengan en el sistema algunas localizaciones específicas. Esto reducirá el espacio de disco consumido en `/usr/share/locale`.

- Mueva de forma temporal a otro sistema o elimínelos de forma permanente, los registros del sistema que residen en `/var/log/`.
- Utilice una ubicación temporal para `/var/cache/apt/archives`: puede utilizar una caché temporal en otro sistema de archivos (USB, dispositivo de almacenamiento, espacio en disco duro temporal, sistema de ficheros en uso, etc.).

NOTA

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

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

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

```
# apt clean
```

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

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

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

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

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

```
# umount /media/usbkey/archives
```

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

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

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

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

4.4.4. Actualización mínima del sistema

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

Para hacer esto, ejecute primero lo siguiente:

```
# apt-get upgrade
```

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

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

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

4.4.5. Actualizar el sistema

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

```
# apt full-upgrade
```

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

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

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

4.5. Posibles problemas durante o después de la actualización

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

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

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

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

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

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

4.5.2. Eliminaciones esperadas

El proceso de actualización a buster 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 buster en Sección 4.8.

4.5.3. Bucles en Conflictos o Pre-Dependencias

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

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

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

para eliminar algunos de los paquete problemáticos, o

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

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

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

4.5.4. Conflictos de archivo

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

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

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

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

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

4.5.5. Cambios de configuración

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

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

4.5.6. Cambio de la sesión en consola

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

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

4.6. Actualización de su núcleo y paquetes relacionados

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

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

4.6.1. Instalación de un metapaquete del núcleo

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

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

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

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

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

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

Luego debería usar `apt install` para instalarlo. Debería reiniciar en cuanto le sea posible una vez que haya instalado el núcleo nuevo para empezar a beneficiarse de las características que proporciona la nueva versión del núcleo. Sin embargo, debe leer primero Sección 5.1.13 antes de hacer el primer reinicio tras una actualización.

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

Siempre que sea posible, es mejor para usted si actualiza el paquete del núcleo de forma independiente a la actualización principal con `full-ugprade`, para así reducir las posibilidades de tener durante

un cierto periodo de tiempo un sistema que no se puede iniciar. Tenga en cuenta que solo debería hacer esto después de haber realizado el proceso de actualización mínima del sistema que se describe en Sección 4.4.4.

4.7. Prepararse para la siguiente distribución

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

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

4.7.1. Purgando los paquetes eliminados

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

ATENCIÓN

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

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

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

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

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

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

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

4.8. Paquetes obsoletos

La versión buster, aunque introduce muchos paquetes nuevos, también retira o deja de distribuir algunos paquetes que estaban disponibles en stretch. 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 buster[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.

[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.

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 buster debido a los errores que presentan. En este último caso los paquetes puede que sigan estando presentes en la distribución "inestable".

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

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

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

Puede consultar una lista de los paquetes obsoletos de Buster en Sección 5.1.11.

4.8.1. Paquetes «dummy» de transición

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

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

Capítulo 5

Problemas que debe tener en cuenta para buster

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

5.1. Actualizar elementos específicos para buster

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

5.1.1. s390x ISA incrementado a z196

La línea base de ISA para la adaptación a `s390x` se ha incrementado a z196. Esto permite que Debian proporcione soporte a paquetes como `rust`, `go` y `nodejs`, que no soportan a ISAs más antiguos.

Como consecuencia de este cambio no debería actualizar a buster si tiene una CPU más antigua.

5.1.2. Opción de montaje hidepid de procfs no soportada

Se han detectado ciertos problemas con las opción de montaje `hidepid` para `/proc` y las versiones recientes de systemd, los desarrolladores de systemd consideran ésta una configuración no soportada. Se recomienda a los usuarios que han modificado `/etc/fstab` para activar estas opciones que las deshabiliten antes de la actualización, para asegurar que las sesiones login funcionen en buster. (Una alternativa posible para re-activarlas está descrita en la página del wiki Hardening (`https://wiki.debian.org/Hardening#Mounting_.2Fproc_with_hidepid`).)

5.1.3. ypbind no puede iniciarse con -no-dbus

Las opciones por omisión de `ypbind` han cambiado. Sin embargo, si ha modificado este archivo los valores anteriores no se actualizarán y debe asegurarse de que la opción `YPBINDARGS=` en `/etc/default/nis` no incluye `-no-dbus`. Si la opción `-no-dbus` está presente, **ypbind** no podrá arrancar y es posible que no pueda acceder al sistema. Para más información consulte la errata bug #906436 (`https://bugs.debian.org/906436`).

5.1.4. NIS server does not answer NIS client requests by default

The default behavior of `rpcbind` has changed to no longer answer remote calls from NIS clients. On NIS servers you will need to add the (Debian-specific) `-r` flag to the command line options of **rpcbind**, otherwise users will not be able to log into your NIS client machines. For more info see bug #935492 (`https://bugs.debian.org/935492`).

5.1.5. sshd falla al autenticar

Las semánticas de las opciones `PubkeyAcceptedKeyTypes` y `HostbasedAcceptedKeyTypes` de `sshd` han cambiado. Estas opciones ahora especifican los algoritmos de firma que se aceptan por los respectivos mecanismos de autenticación, mientras que antes especificaban los tipos de clave aceptados. Esta distinción es importante cuando se utiliza el algoritmo de firma RSA/SHA2 `rsa-sha2-256`, `rsa-sha2-512` y sus certificados equivalentes. Las configuraciones que sobreescriben estas opciones pero omiten los nombres de estos algoritmos pueden causar fallos de autenticación inesperados.

No se requiere una acción para las configuraciones que aceptan los valores por omisión para estas opciones.

5.1.6. Los demonios no arrancan o el sistema parece colgarse durante el arranque

El sistema puede bloquearse durante minutos e incluso hors si el susbistema de información aleatoria no está suficientemente inicializado (`random: crng init done`). Esto sucede debido a la necesidad de `systemd` e entropía durante el arranque y el núcleo tratando estas llamadas como bloqueantes cuando la entropía disponible es baja. Para sistemas `amd64` que soportan la instrucción `RDRAND` este problema se puede evitar si el núcleo de Debian utiliza esta instrucción por omisión (`CONFIG_RANDOM_TRUST_CPU`).

Los sistemas que no sean `amd64` y algunos tipos de máquinas virtuales y algunos tipos de máquinas virtuales deben disponer de diferentes fuentes de entropía para poder arrancar rápidamente. El programa `haveged` ha sido elegido para ésto por el proyecto del Instalador de Debian y puede ser una opción válida si no hay entropía hardware en el sistema. En máquinas virtuales puede considerar reenviar la entropía del huésped a la máquina virtual a través de `virtio_rng`.

Si lee esto después de actualizar a sistemas remotos de buster, envíe pings al sistema en la red de forma contínua puesto que ésto añade entropía a la fuente de información aleatoria y el sistema será alcanzable por ssh de nuevo.

Consulte el wiki (`https://wiki.debian.org/BoottimeEntropyStarvation`) y al resumen de DLange de este problema (`https://daniel-lange.com/archives/152-hello-buster.html`) para ver más opciones.

5.1.7. Migración de los nombres de interfaz de red antiguos

Si su sistema se actualizó de una versión anterior y aún utiliza los nombres de interfaces de red antiguos que quedaron obsoletos en stretch (como `eth0` o `wlan0`), debería tener en cuenta que el mecanismo de definir sus nombres a través de `/etc/udev/rules.d/70-persistent-net.rules` ya no está soportado oficialmente por `udev` en buster (aunque puede funcionar en algunos casos). Para evitar el problema de que su equipo pierda conectividad durante la actualización de buster, se recomienda que migre de forma anticipada al nuevo esquema de nombres (habitualmente esto significa utilizar los nombres como `enp0s1` o `wlp2s5`, que incorporan nombre del bus PCI y números d eranura). Tenga cuidado de actualizar cualquier nombre de interfaz que se haya introducido en otros elementos de configuración como cortafuegos, `ifupdown`, etc.

The alternative is to switch to a supported mechanism for enforcing the old naming scheme, such as a systemd `.link` file (see systemd.link(5) (`https://manpages.debian.org/buster/systemd.link`)). The `net.ifnames=0` kernel commandline option might also work for systems with only one network interface (of a given type).

Para encontrar los nombres del nuevo formato que se van a utilizar debe primero encontrar los nombres actuales de los interfaces relevantes:

```
$ echo /sys/class/net/[ew]*
```

Para cada uno de estos nombres, compruebe si se están utilizando en los archivos de configuración y qué nombre `udev` prefiere utilizar para ellos:

```
$ sudo rgrep -w eth0 /etc
$ udevadm test-builtin net_id /sys/class/net/eth0 2>/dev/null
```

This should give enough information to devise a migration plan. (If the `udevadm` output includes an "onboard" or "slot" name, that takes priority; MAC-based names are normally treated as a fallback, but may be needed for USB network hardware.)

Una vez esté preparado para hacer el cambio, deshabilite `70-persistent-net.rules` bien renombrándolo o bien comentando las líneas individuales. En máquinas virtuales tiene que eliminar los archivos `/etc/systemd/network/99-default.link` y (si utiliza interfaces de red virtio) `/etc/systemd/network/50-virtio-kernel-names.link`. Después reconstruya `initrd`:

```
$ sudo update-initramfs -u
```

y reinicie. Su sistema debería utilizar ahora los nombres de interfaces en el nuevo estilo. Ajuste cualquier configuración pendiente y vuelva a probar su sistema.

See the wiki (`https://wiki.debian.org/NetworkInterfaceNames`), upstream documentation (`https://www.freedesktop.org/software/systemd/man/systemd.net-naming-scheme.html`), and the `udev README.Debian` for further information.

5.1.8. Configuración de módulos para interfaces agrupados y «dummy»

Los sistemas que utilizan interfaces con canales agrupados o «dummy», como por ejemplo en los sistemas que están configurados como enrutadores, pueden tener problemas durante la actualización a buster. Las nuevas versiones de `systemd` instalan un archivo `/lib/modprobe.d/systemd.conf` (dirigido a simplificar la configuración via **systemd-networkd**) que contiene las líneas

```
options bonding max_bonds=0
options dummy numdummies=0
```

Los administradores que dependen de valores distintos tienen que asegurarse que están definidos de la forma correcta para que tengan precedencia. Un archivo en `/etc/modprobe.d` tendrá precedencia sobre el mismo nombre bajo `/lib/modprobe.d`, pero los nombres se procesan en orden alfabético, por lo que `/lib/modprobe.d/systemd.conf` sigue y tiene precedencia sobre (por ejemplo) `/etc/modprobe.d/dummy.conf`. Asegúrese de que cualquier archivo de configuración local tiene un nombre que quede ordenado después de "`systemd.conf`", como "`/etc/modprobe.d/zz-local.conf`".

5.1.9. Versión por omisión de OpenSSL e incremento del nivel de seguridad

Siguiendo distintas recomendaciones de seguridad, la versión mínima de TLS por omisión se ha modificado de TLSv1 a TLSv1.2.

El nivel de seguridad por omisión de conexiones TLS se ha incrementado también de nivel 1 a nivel 2. Esto mueve el nivel de seguridad de 80 a 112 bits, y hace necesario utilizar claves RSA y DHE de 2048 o más bits, claves ECC de 224 o más bits, y SHA-2.

Los valores configurados para todo el sistema pueden modificarse en `/etc/ssl/openssl.cnf`. Algunas aplicaciones pueden tener también una forma específica para la aplicación para cambiar estos valores por omisión.

En el archivo de configuración `/etc/ssl/openssl.cnf` hay una línea `MinProtocol` y `CipherString`. El valor de `CipherString` también puede definir el nivel de seguridad. Puede encontrar información de los niveles de seguridad en la página de manual SSL_CTX_set_security_level(3ssl) (`https://manpages.debian.org/buster/SSL_CTX_set_security_level(3ssl)`). La lista de cadenas válida para la versión mínima del protocolo pueden encontrarse en SSL_CONF_cmd(3ssl) (`https://manpages.debian.org/buster/SSL_CONF_cmd(3ssl)`). Puede encontrar más información en ciphers(1ssl) (`https://manpages.debian.org/buster/ciphers(1ssl)`) y config(5ssl) (`https://manpages.debian.org/buster/config(5ssl)`).

Puede modificar los valores por omisión del sistema a los valores anteriores cambiando `/etc/ssl/openssl.cnf` como se indica a continuación:

```
        MinProtocol = None
        CipherString = DEFAULT
```

Se recomienda que contacte con el sitio remoto si los valores por omisión provocan problemas.

5.1.10. Algunas aplicaciones no funcionan con GNOME en Wayland

GNOME en buster ha cambiado su servidor de pantalla por omisión de Xorg a Wayland (consulte Sección 2.2.11). Algunas aplicaciones no se han actualizado para funciona correctamente en Wayland, esto incluye el popular gestor de paquetes `synaptic`, el método de entrada de chino simplificado, `fcitx`, y la mayor parte de las herramientas para grabacin̂ de pantalla. Debe acceder en una sesión `GNOME en Xorg` si quiere utilizar estos programas.

5.1.11. Paquetes obsoletos notables

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

La lista de paquetes obsoletos incluye:

- Ya no se da soporte al paquete `mcelog` con las versiones del núcleo superiores a la 4.12. Puede utilizar `rasdaemon` como sustituto.
- Ya no se incluye al paquete `revelation`, utilizado para almacenar contraseñas, en buster. `keepass2`puede importar los archivos de contraseñas XML previamente exportados de `revelation`. Asegúrese de exportar los datos de revelation antes de actualizar para evitar perder acceso a sus contraseñas.
- El paquete `phpmyadmin` no está incluido en buster.
- Se ha eliminado de buster `ipsec-tools` y `racoon` porque el código fuente no está actualizándose suficientemente rápido y no está adaptado a nuevas amenazas.

  Se recomienda a los usuarios a migrar a `libreswan`, que tiene un compatibilidad de protocolos más amplia y está manteniéndose de forma activa por sus desarrolladores.

  El paquete `libreswan` debería ser totalmente compatible en términos de protocolos de comunicación dado que implementa un superconjunto de los protocolos soportados por `racoon`.
- El MTA sencillo `ssmtp` ya no se distribuye en buster. Esto se debe a que no valida actualmente certificados TLS. Para más información consulte bug #662960 (`https://bugs.debian.org/662960`).
- El paquete `ecryptfs-utils` no es parte de buster debido a una errata serie que aún no está arreglada (#765854 (`https://bugs.debian.org/765854`)). En el momento de escribir estas líneas no hay una recomendación disponible para los usuarios de eCryptfs, excepto no actualizar.

5.1.12. Componentes obsoletos de buster

Con la publicación de Debian 11 (nombre en clave bullseye) algunas funcionalidades estarán obsoletas. Los usuarios deben migrar a otras alternativas para evitar problemas al actualizar a Debian 11.

Esto incluye las siguientes funcionalidades:

- Python 2 dejará de estar soportado por sus desarrolladores el 1 de enero del 2020 (`https://www.python.org/dev/peps/pep-0373/`). Debian espera dejar de distribuir `python-2.7` en Debian 11. Los usuarios que tienen funcionalidades que dependen de **python** deberían preparar la migración a **python3**.
- Icinga 1.x está fuera de soporte por los desarrolladores principales desde el 31 de diciembre de 2018. Mientras el paquete `icinga` esté instalado los usuarios pueden utilizar el ciclo de vida de buster para migrar a Icinga 2 (`icinga2`) y a Icinga Web 2 (`icingaweb2`). El paquete `icinga2-classicui` aún está disponible para usar la interfaz CGI web de Icinga 1.x CGI con Icinga 2, pero se va a eliminar el soporte de esta interfaz en Icinga 2.11. Debería utilizarse Icinga Web 2 en su lugar.
- El gestor de listas Mailman versión 3 es una novedad de esta publicación. Se ha dividido mailman en distintos componentes: el componente core está disponible en el paquete `mailman3` y el conjunto completo puede obtenerse a través del metapaquete `mailman3-full`.

La versión antigua 2.1 de Mailman está aún disponible en esta publicación en el paquete `mailman`. Puede migrar una instalación existente a la nueva versión cuando lo desee. Se mantendrá el paquete versión 2.1 de Mailman en el futuro cercano, pero no se introducirán cambios importantes ni mejoras. Este paquete se eliminará de la primera publicación de Debian que se realice después de que los desarrolladores de Mailman dejen de dar soporte a esta rama.

Se recomienda a todos que actualicen a Mailman 3, la versión más reciente y que está desarrollándose de forma activa.

- Los paquetes `spf-milter-python` y `dkim-milter-python` ya no están siendo mantenidos por los desarrolladores originales. Pero sus reemplazos `pyspf-milter` y `dkimpy-milter` tienen más funcionalidades y están disponibles en buster. Los usuarios debería migrar a los nuevos paquetes antes de que los antiguos se eliminen en bullseye.

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

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

5.1.14. Los paquetes relacionados con SysV init ya no son necsearios

NOTA

Esta sección no aplica si ha decidido continuar utilizando sysvinit-core.

Después de haber cambiado a systemd como sistema de arranque por omisión en Jessie, y las mejoras realizadas en Strecth, ya no es necesario tener instalados algunos paquetes relacionados con SysV. Estos paquetes pueden borrarse de forma segura como sigue

```
apt purge initscripts sysv-rc insserv startpar
```

5.2. Limitaciones en el soporte de seguridad

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

NOTA

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

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

Debian 10 incluye varios motores de navegadores web que están afectados por un flujo constante de vulnerabilidades de seguridad. La alta tasa de vulnerabilidades y la falta de un soporte por parte de los desarrolladores a versiones anteriores hace muy difícil dar soporte a estos navegadores y motores con arreglos de seguridad preparados para las versiones distribuidas. Además, las interdependencias entre bibliotecas hacen extremadamente díficil actualizar a las nuevas versiones distribuidas. Por tanto, los

navegadores basados p.ej. en los motores de webkit y khtml[1] están incluidos en buster, pero no están cubiertos por el soporte completo de seguridad. No deberían utilizarse estos navegadores para acceder a sitios no confiables. El paquete fuente `webkit2gtk` está cubierto por el soporte de seguridad.

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

5.2.2. Paquetes basados en Go

La infrastructura de Debian no proporciona soporte a gran escala para la reconstrucción de paquetes que enlazan de forma estática con otros paquetes. Hasta buster esto no ha sido un problema en la práctica, pero con el crecimiento del ecosistema de Go esto significa que los paquetes basados en Go no están cubiertos por el soporte regular de seguridad. Estarán cubiertos cuando se mejore la infrastructura se actualice y mejore para poder gestionarlos de una forma mantenible.

Si es necesario producir una actualización, éstas sólo pueden ofrecerse a través de una nueva publicación, que tardará un tiempo en producirse.

5.3. Problemas específicos de paquetes

La actualización de los paquetes entre stretch y buster debería ser esencial en la mayoría de los casos. Existe un pequeño número de casos en los que es necesaria una intervención manual, bien antes o bien después de la actualización. Estos casos se detallan a continuación para cada paquete.

5.3.1. Cambio en las semánticas del uso de variables de entorno para su

Se han modificado las semánticas de `su` en buster y el programa ya no mantiene las variables del entorno de usuario `DISPLAY` y `XAUTHORITY`. Tendrá que fijar explícitamente estas variables si desea ejecutar aplicaciones gráficas con `su`. Puede leer una discusión extensiva sobre este comportamiento en bug #905409 (`https://bugs.debian.org/905409`).

5.3.2. Reindexación necesaria en bases de datos PostgreSQL existentes

Los datos de localización de `glibc` se actualizarán cuando se actualice de stretch a buster. Específicamente, esto modifica como PostgreSQL ordena los datos en texto en los índices. Para evitar corrupción de datos, estos índices tienen que `REINDEX`arse inmediatamente después de actualizar los paquetes `locales` o `locales-all` y en cualquier caso antes de poner la base de datos de nuevo en producción.

Orden sugerida

```
sudo -u postgres reindexdb --all
```

Alternativamente, actualice la base de datos a PostgreSQL 11 utilizando **pg_upgradecluster**. (Este utiliza por omisión **pg_dump** que reconstruye todos los índices. *No* es seguro utilizar la opción `-m upgrade` o **pg_upgrade** porque mantienen el orden incorrecto de los índices.)

Consulte el Wiki de PostgreSQL Wiki (`https://wiki.postgresql.org/wiki/Locale_data_changes`) para más información.

5.3.3. mutt y neomutt

En stretch, el paquete `mutt` tiene parches aplicados de las fuentes de https://neomutt.org (`https://neomutt.org`). A partir de buster, el paquete que ofrece `/usr/bin/mutt` incluirá en su lugar las fuentes originales de http://www.mutt.org (`http://www.mutt.org`), y se ofrece un paquete separado `neomutt` que ofrece `/usr/bin/neomutt`.

Esto significa que algunas de las funcionalidades que estaban disponibles previamente en `mutt`. Si esto rompe su configuración puede instalar `neomutt` en su lugar.

[1] Estos motores se distribuyen con un número diferente de paquetes fuente y la problemática aplica a todos los paquetes que los incluyen. Estos problemas también se extenden a los montores de render web que no se mencionen aquí explícitamente, con la excepción de `webkit2gtk`.

5.3.4. Acceso de la configuración de GNOME sin ratón

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

5.3.5. gnome-disk-utility fails to change LUKS password causing permanent data loss (buster 10.0 only)

Users of the initial buster release images should not change the LUKS password of encrypted disks with the GNOME graphical interface for disk management. The `gnome-disk-utility` package in buster had a very nasty bug (#928893) (`https://bugs.debian.org/928893`) when used to change the LUKS password: it deleted the old password but failed to correctly set the new one, making all data on the disk inaccessible. This has been fixed in the first point release.

5.3.6. evolution-ews se ha eliminado, y se eliminarán los buzones de correo que utilicen Exchange, Office365 o un servidor de Outlook

Los usuarios que utilicen como su cliente de correo `evolution` y se conecten a un servidor ejecutando Exchange, Office365 o Outlook con el complemento `evolution-ews` no deberían actualizarse a buster sin guardar sus datos y sin tener disponible una solución alternativa de antemano. El complemento evolution-ews se ha eliminado debido a la errata #926712 (`https://bugs.debian.org/926712`) y, si se actualizan, perderán acceso a sus buzones personales, calendario, listas de contactos y tareas y no podrá acceder a ellos con Evolution.

The `evolution-ews` package has been reintroduced via buster-backports. Users upgrading from stretch to buster can enable buster-backports after the upgrade and then they will be able to reinstall `evolution-ews`.

5.3.7. El instalador Calamares deja claves de cifrado de disco legibles

Cuando se instala Debian desde los medios «live» con el instalador de Calamares (Sección 2.2.13) y seleccionan la funcionalidad de cifrado completo de disco, la clave de desbloqueo del disco se guarda en initramfs que puede ser leída por cualquier usuario. Esto permite que los usuarios que tengan acceso al sistema de fichero local puedan leer la clave privada y obtener acceso al sistema de ficheros en el futuro.

Esto puede evitarse añadiendo `UMASK=0077` a `/etc/initramfs-tools/conf.d/initramfs-permissions` y ejecutando **update-initramfs -u**. Esto generará un nuevo initramfs sin los permisos de lectura universales.

Se ha planeado un arreglo para el instalador (consulte la errata #931373 (`https://bugs.debian.org/931373`)) y se subirá a debian-security. Mientras tanto, los usuarios del cifrado completo de disco deben aplicar la configuración descrita anteriormente.

5.3.8. S3QL URL changes for Amazon S3 buckets

When using `s3ql` with Amazon S3 buckets, the configuration needs updating for a change in the URL. The new format is:

```
s3://<region>/<bucket>/<prefix>
```

5.3.9. Split in configuration for logrotate

The shipped configurations for `/var/log/btmp` and `/var/log/wtmp` have been split from the main configuration file (`/etc/logrotate.conf`) into separate standalone files (`/etc/logrotate.d/btmp` and `/etc/logrotate.d/wtmp`).

If you have modified `/etc/logrotate.conf` in this regard, make sure to re-adjust the two new files to your needs and drop any references to (b|w)tmp from the main file, since duplicate definitions can cause errors.

5.3.10. The `rescue` boot option is unusable without a root password

With the implementation of `sulogin` now used, booting with the `rescue` option always requires the root password. If one has not been set, this makes the rescue mode effectively unusable. However it is still possible to boot using the kernel parameter `init=/sbin/sulogin --force`

To configure systemd to do the equivalent of this whenever it boots into rescue mode (also known as single mode: see systemd(1) (`https://manpages.debian.org/buster//buster/systemd/systemd.1.html`)), run **sudo systemctl edit rescue.service** and create a file saying just:

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

It might also (or instead) be useful to do this for the `emergency.service` unit, which is started *automatically* in the case of certain errors (see systemd.special(7) (`https://manpages.debian.org/buster//buster/systemd/systemd.special.7.html`)), or if `emergency` is added to the kernel command line (e.g. if the system can't be recovered by using the rescue mode).

For background and a discussion on the security implications see #802211 (`https://bugs.debian.org//802211`).

Capítulo 6

Más información sobre Debian

6.1. Para leer más

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

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

6.2. Cómo conseguir ayuda

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

6.2.1. Listas de correo electrónico

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

6.2.2. Internet Relay Chat (IRC)

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

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

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

6.3. Cómo informar de fallos

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

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

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

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

6.4. Cómo colaborar con Debian

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

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

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

Capítulo 7

Glosario

ACPI

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

ALSA

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

BD

Disco Blu-ray

CD

Disco compacto

CD-ROM

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

DHCP

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

DLBD

Disco Blu-ray de doble capa

DNS

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

DVD

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

GIMP

Programa de Manipulación de Imágenes de GNU

GNU

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

GPG

GNU Privacy Guard

LDAP

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

LSB

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

LVM

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

MTA

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

NBD

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

NFS

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

NIC

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

NIS

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

PHP

PHP: Preprocesador de Hipertexto

RAID

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

SATA

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

SSL

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

TLS

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

UEFI

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

USB

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

UUID

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

WPA

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

Apéndice A

Gestión de su sistema stretch antes de la actualización

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

A.1. Actualizar su sistema stretch

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

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

A.2. Comprobar su lista de fuentes APT

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

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

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

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 stretch o de buster.

IMPORTANTE

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

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

```
# apt update
```

para actualizar la lista de paquetes.

A.3. Borrar ficheros de configuración obsoletos

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

A.4. Actualización de localizaciones antiguas a UTF-8

El uso de las localizaciones antiguas no-UTF-8 han dejado de estar soportadas hace mucho tiempo tanto por los entornos de escritorio como por otros projectos importantes. Estas localizaciones deberían actualizarse ejecutando **dpkg-reconfigure locales** y seleccionando una localización UTF-8 como valor por omisión. Debería también asegurarse que los usuarios no cambian el valor por omisión utilizando una localización obsoleta en su entorno.

Apéndice B

Personas que han contribuido a estas notas de publicación

Hay muchas personas que han ayudado con estas notas de publicación, incluyendo, entre otros, a

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

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

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

Índice alfabético

A
Apache, 4

B
BIND, 4

C
Calligra, 3
Cryptsetup, 4

D
DocBook XML, 2
Dovecot, 4

E
Evolution, 4
Exim, 4

G
GCC, 4
GIMP, 4
GNOME, 3
GNUcash, 3
GnuPG, 4

I
Inkscape, 4

K
KDE, 3

L
LibreOffice, 3
LXDE, 3
LXQt, 3

M
MariaDB, 4
MATE, 3

N
Nginx, 4

O
OpenJDK, 4
OpenSSH, 4

P
packages
- apparmor, 5
- apparmor-profiles-extra, 5
- apt, 2
- apt-listchanges, 21
- aptitude, 14, 19, 24
- cryptsetup, 6
- cups, 7
- cups-browsed, 7
- cups-filters, 6
- dblatex, 2
- debian-goodies, 19
- debian-kernel-handbook, 23
- debian-security-support, 31
- dkim-milter-python, 31
- dkimpy-milter, 31
- doc-debian, 36
- docbook-xsl, 2
- dpkg, 2
- ecryptfs-utils, 30
- evince, 5
- evolution, 33
- evolution-ews, 33
- fcitx, 30
- gnome-control-center, 33
- gnome-disk-utility, 33
- go, 27
- grub-efi-amd64-signed, 4
- grub-efi-ia32-signed, 4
- haveged, 28
- how-can-i-help, 36
- icinga, 30
- icinga2, 30
- icinga2-classicui, 30
- icingaweb2, 30
- ifupdown, 28
- initramfs-tools, 12, 23
- ipsec-tools, 30
- iptables, 5
- keepass2, 30
- libreswan, 30
- linux-image-*, 23
- linux-image-amd64, 23
- linux-source, 23
- localepurge, 19
- locales, 32
- locales-all, 32
- mailman, 31
- mailman3, 30
- mailman3-full, 30
- manpages-de, 5
- mcelog, 30
- mutt, 5, 32
- neomutt, 32
- nodejs, 27
- phpmyadmin, 30
- popularity-contest, 19
- pyspf-milter, 31
- python-2.7, 30
- racoon, 30
- rasdaemon, 30
- release-notes, 1
- revelation, 30
- rpcbind, 27
- rust, 27
- s3ql, 33

shim-signed, 4
spf-milter-python, 31
sshd, 28
ssmtp, 30
synaptic, 14, 30
systemd, 5, 28, 29
tinc, 13
udev, 23, 28
unattended-upgrades, 5
upgrade-reports, 2
usrmerge, 7
util-linux, 5
xmlroff, 2
xsltproc, 2
ypbind, 27
Perl, 4
PHP, 4
Postfix, 4
PostgreSQL, 4

X
Xfce, 3