Note de lansare pentru Debian 11 (bullseye), 32-bit MIPS (little endian)

Proiectul de documentare Debian (https://www.debian.org/doc/)

17 aprilie 2024
Note de lansare pentru Debian 11 (bullseye), 32-bit MIPS (little endian)

Acest document este software liber și poate fi redistribuit și/sau modificat conform termenilor licenței GNU General Public License, versiunea 2, așa cum a fost publicată de Free Software Foundation.

Acest program este distribuit cu speranța că va fi util, dar FĂRĂ NICI O GARANȚIE, nici chiar garanția implicită de VANDABILITATE sau POTRIVIRE CU UN ANUMIT SCOP. A se vedea licența GNU General Public License pentru mai multe detalii.

Ar fi trebuit să primiți o copie a licenței GNU General Public License împreună cu acest program. În caz contrar scrieți la Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Textul licenței se găsește și la https://www.gnu.org/ licences/gpl-2.0.html și /usr/share/ common-licenses/GPL-2 pe sisteme Debian.
Cuprins

1 Introducere
   1.1 Raportarea problemelor din acest document .......................... 1
   1.2 Contribuirea cu rapoarte de instalare .................................. 1
   1.3 Sursele acestui document .................................................. 2

2 Noutăți în Debian 11
   2.1 Arhitecturi suportate ..................................................... 3
   2.2 Noutăți în distribuție ..................................................... 3
      2.2.1 Desktops and well known packages .................................. 3
      2.2.2 Driverless scanning and printing ................................. 4
         2.2.2.1 CUPS and driverless printing .................................. 4
         2.2.2.2 SANE and driverless scanning ................................. 5
      2.2.3 New generic open command ......................................... 5
      2.2.4 Control groups v2 .................................................... 5
      2.2.5 Persistent systemd journal ........................................ 5
      2.2.6 New Fcitx 5 Input Method ......................................... 5
      2.2.7 Noutăți de la Blend-ul Debian Med ................................ 5
      2.2.8 Kernel support for exFAT ........................................... 6
      2.2.9 Improved man page translations ................................. 6
      2.2.10 Improved support for alternative init systems .................. 6
      2.2.11 Initial availability of the Bazel build system ................. 6

3 Sistemul de instalare ......................................................... 7
   3.1 Ce este nou în sistemul de instalare? .................................. 7
      3.1.1 Help with installation of firmware ................................ 7
      3.1.2 Instalarea automată .................................................. 7
   3.2 Container and Virtual Machine images .................................. 8

4 Actualizarea de la Debian 10 (buster) ....................................... 9
   4.1 Pregătirile pentru actualizare ....................................... 9
      4.1.1 Faceți copii de siguranță pentru orice date sau configurații .... 9
      4.1.2 Informații utilizatorii din timp ................................... 9
      4.1.3 Pregătiri pentru indisponibilitatea serviciilor .................... 9
      4.1.4 Pregătiri pentru recuperare ....................................... 10
         4.1.4.1 Consolă de depanare în timpul inițializării folosind initrd .... 10
         4.1.4.2 Consolă de depanare în timpul inițializării folosind systemd ... 11
      4.1.5 Pregătiți un mediu sigur pentru actualizare ..................... 11
   4.2 Start from „pure” Debian ................................................. 11
      4.2.1 Upgrade to Debian 10 (buster) .................................... 11
      4.2.2 Remove non-Debian packages ....................................... 11
      4.2.3 Upgrade to latest point release ................................... 12
      4.2.4 Prepare the package database ..................................... 12
      4.2.5 Remove obsolete packages ......................................... 12
      4.2.6 Clean up leftover configuration files ............................. 12
      4.2.7 The security section ............................................... 12
      4.2.8 Sectiona proposed-updates ....................................... 12
      4.2.9 Surse nooficiale .................................................... 12
      4.2.10 Dezactivarea alegerilor selective APT ............................ 13
      4.2.11 Check package status ............................................. 13
   4.3 Pregătirea sursei pentru APT ........................................... 13
      4.3.1 Adăugarea de surse internet pentru APT ......................... 14
      4.3.2 Adăugarea de surse APT pentru un sit-oglindă local ............ 14
      4.3.3 Adăugarea de surse APT de pe un mediu optic .................. 15
   4.4 Actualizarea pachetelor .................................................. 15
5 Probleme în bullseye de care ar trebui să știți

5.1 Elemente specifice actualizării la bullseye

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.1 The XFS file system no longer supports barrier/nobarrier option</td>
<td>23</td>
</tr>
<tr>
<td>5.1.2 Changed security archive layout</td>
<td>23</td>
</tr>
<tr>
<td>5.1.3 Password hashing uses yescrypt by default</td>
<td>23</td>
</tr>
<tr>
<td>5.1.4 NSS NIS and NIS+ support require new packages</td>
<td>24</td>
</tr>
<tr>
<td>5.1.5 Config file fragment handling in unbound</td>
<td>24</td>
</tr>
<tr>
<td>5.1.6 rsync parameter deprecation</td>
<td>24</td>
</tr>
<tr>
<td>5.1.7 Vim addons handling</td>
<td>24</td>
</tr>
<tr>
<td>5.1.8 OpenStack and cgroups v1</td>
<td>24</td>
</tr>
<tr>
<td>5.1.9 OpenStack API policy files</td>
<td>24</td>
</tr>
<tr>
<td>5.1.10 sendmail downtime during upgrade</td>
<td>25</td>
</tr>
<tr>
<td>5.1.11 FUSE 3</td>
<td>25</td>
</tr>
<tr>
<td>5.1.12 GnuPG options file</td>
<td>25</td>
</tr>
<tr>
<td>5.1.13 Linux enables user namespaces by default</td>
<td>25</td>
</tr>
<tr>
<td>5.1.14 Linux disables unprivileged calls to bpf() by default</td>
<td>25</td>
</tr>
<tr>
<td>5.1.15 redmine missing in bullseye</td>
<td>26</td>
</tr>
<tr>
<td>5.1.16 Exim 4.94</td>
<td>26</td>
</tr>
<tr>
<td>5.1.17 SCSI device probing is non-deterministic</td>
<td>26</td>
</tr>
<tr>
<td>5.1.18 rdiff-backup require lockstep upgrade of server and client</td>
<td>26</td>
</tr>
<tr>
<td>5.1.19 Intel CPU microcode issues</td>
<td>27</td>
</tr>
<tr>
<td>5.1.20 Upgrades involving libgc1c2 need two runs</td>
<td>27</td>
</tr>
<tr>
<td>5.1.21 fail2ban can't send e-mail using mail from bsd-mailx</td>
<td>27</td>
</tr>
<tr>
<td>5.1.22 No new SSH connections possible during upgrade</td>
<td>27</td>
</tr>
<tr>
<td>5.1.23 Open vSwitch upgrade requires interfaces(5) change</td>
<td>27</td>
</tr>
<tr>
<td>5.1.24 Operațiuni de executat după actualizare și înainte de repornire.</td>
<td>27</td>
</tr>
<tr>
<td>5.2 Items not limited to the upgrade process</td>
<td>27</td>
</tr>
<tr>
<td>5.2.1 Limitări în suportul de securitate</td>
<td>27</td>
</tr>
<tr>
<td>5.2.1.1 Starea securității navigatoarelor web și a motoarelor de randare</td>
<td>28</td>
</tr>
<tr>
<td>5.2.1.2 OpenJDK 17</td>
<td>28</td>
</tr>
<tr>
<td>5.2.1.3 Go-based packages</td>
<td>28</td>
</tr>
<tr>
<td>5.2.2 Accesarea setărilor GNOME fără mouse</td>
<td>28</td>
</tr>
<tr>
<td>5.2.3 The rescue boot option is unusable without a root password</td>
<td>28</td>
</tr>
<tr>
<td>5.2.4 32-bit Xen PV guests are not supported</td>
<td>29</td>
</tr>
<tr>
<td>5.3 Obsolescence and deprecation</td>
<td>29</td>
</tr>
<tr>
<td>5.3.1 Pachete notabile învechite</td>
<td>29</td>
</tr>
<tr>
<td>5.3.2 Componente depășite din bullseye</td>
<td>30</td>
</tr>
<tr>
<td>5.4 Known severe bugs</td>
<td>30</td>
</tr>
</tbody>
</table>
6 Mai multe informații despre Debian 33
   6.1 Referințe suplimentare ........................................... 33
   6.2 Obținerea de ajutor .................................................. 33
      6.2.1 Listele de discuții ............................................ 33
      6.2.2 Internet Relay Chat ........................................... 33
   6.3 Raportarea problemelor ............................................ 33
   6.4 Contribuirea la Debian ............................................. 34

7 Glosar 35

A Gestionarea sistemului buster înainte de actualizare 37
   A.1 Actualizarea sistemului buster .................................. 37
   A.2 Verificarea fișierelor listelor de surse APT ....................... 37
   A.3 Îndepărtarea fișierelor de configurare inutile .................... 38

B Contribuitorii la Notele de lansare 39

Glosar 41
Capitolul 1

Introducere

Acest document informează utilizatorii distribuției Debian despre schimbările majore din versiunea 11 (cu nume de cod bullseye).

Notele de lansare oferă informații despre cum se poate actualiza în siguranță de la versiunea 10 (cu nume de cod buster) la versiunea curentă și informează utilizatorii despre poențiale probleme ce pot fi întâlnite în decursul actualizării.

You can get the most recent version of this document from https://www.debian.org/releases/bullseye/releasenotes.

ATENȚIE

Țineți cont că este imposibil să menționăm toate problemele cunoscute și de aceea s-a făcut o selecție pe baza preponderenței și impactului așteptat.

Vă rugăm să țineți cont că suportăm doar actualizări de la Debian versiunea precedentă (în acest caz actualizări de la buster). În cazul în care trebuie să actualizați de la versiuni mai vechi vă sugerăm să citiți edițiile precedente ale noteor de lansare și să actualizați mai întâi la buster.

1.1 Raportarea problemelor din acest document

Am încercat să testăm toți pașii descriși în acest document și să anticipăm toate posibile probleme pe care utilizatorii noștri le-ar putea întâmpina.


Apreciem și încurajăm rapoarte care conțin și un patch (n. trad. petic) pentru sursele documentului. Veți găsi mai multe informații despre cum se obțin sursele acestui document în Secțiune 1.3.

1.2 Contribuirea cu rapoarte de instalare

Orice informații de la utilizatori despre actualizări de la buster la bullseye sunt binevenite. Dacă doriti să contribuiți informații puteți să înregistrați un raport de problemă în sistemul de raportare a problemelor (https://bugs.debian.org/) pentru pachetul upgrade-reports cu rezultatele dumneavoastră.

Vă rugăm comprimați orice atașamente incluse (folosind gzip).

Vă rugăm includeti următoarele informații când trimiteți un raport de actualizare:

• Starea bazei de date cu pachete înainte și după actualizare: baza de date de stare a programului dpkg disponibilă în /var/lib/dpkg/status și baza de date de stare a pachetelor a pachetului

1
apt, disponibilă în /var/lib/apt/extended_states. Ar fi trebuit să faceți o copie de sigură-
ranță înainte de actualizare, după cum e descris în Secțiune 4.1.1, dar puteți găsi copii de siguranță
pentru /var/lib/status în /var/backups.

- Jurnalul sesiunii folosind script, după cum este descris în Secțiune 4.4.1.
- Jurnalele apt, disponibile în /var/log/apt/term.log sau jurnalele aptitude, disponibile în
/var/log/aptitude.

**NOTĂ**

Ar trebui să vă faceți timp să revizuiți jurnalele și să ștergeți orice informații sen-
sibile și/sau confidențiale înainte să le incluiți în raport, deoarece acestea vor fi
publicate într-o bază de dată publică.

### 1.3 Sursele acestui document

Sursele acestui document sunt în format DocBook XML. Versiunea HTML este generată folosind docbook-xsl
și xsltproc. Versiunea PDF este generată folosind dblatex sau xmlroff. Sursele pentru No-
tele de lansare sunt disponibile în depozitul Git al Debian Documentation Project (n. trad. Proiectul
de documentație Debian). Puteți folosi interfața web (https://salsa.debian.org/ddp-team/
release-notes/) pentru a accesa fișierele individuale și să vedeți modificările acestora. Pentru mai
multe informații despre accesarea Git-ului vă rugăm să consultați pagina cu informații despre VCS a
Capitolul 2

Noutăți în Debian 11

Pagina Wiki (https://wiki.debian.org/NewInBullseye) are mai multe informații despre acest subiect.

2.1 Arhitecturi suportate

Următoarele arhitecturi sunt suportate oficial în Debian 11:

- PC pe 32 de biți (i386) și PC pe 64 de biți (amd64)
- ARM pe 64 de biți (arm64)
- ARM EABI (armel)
- ARMv7 (EABI hard-float ABI, armhf)
- little-endian MIPS (mipsel)
- MIPS little-endian pe 64 de biți (mips64el)
- PowerPC little-endian pe 64 de biți (ppc64el)
- IBM System z (s390x)

Puteți să citiți mai multe despre starea portărilor și să aflați detalii specifice arhitecturii dumneavoastră din paginile web ale portărilor Debian (https://www.debian.org/ports/).

2.2 Noutăți în distribuție

Această nouă versiune Debian aduce din nou mult mai mult software decât versiunea precedentă, buster. Distribuția include peste 11294 de pachete noi, ajungând la un total de peste 59551 de pachete. Mare parte din software-ul din distribuție a fost actualizat: peste 42821 de pachete software (adică 72% din numărul de pachete din buster). De asemenea, din diverse motive, un număr semnificativ de pachete (peste 9519, 16% din pachetele din buster) au fost scoase din distribuție. Pentru aceste pachete nu veți mai vedea actualizări, acestea fiind marcate ca „învechite” în interfețele de administrare a pachetelor. Consultați Secțiune 4.8.

2.2.1 Desktops and well known packages

Debian again ships with several desktop applications and environments. Among others it now includes the desktop environments GNOME 3.38, KDE Plasma 5.20, LXDE 11, LXQt 0.16, MATE 1.24, and Xfce 4.16.

Aplicațiile de productivitate au fost de asemenea actualizate, inclusiv suitele de birou:

- LibreOffice is upgraded to version 7.0;
- Calligra is upgraded to 3.2.
• GNUcash is upgraded to 4.4;

Această versiune conține, printre multe altele, și următoarele actualizări:

<table>
<thead>
<tr>
<th>Pachet</th>
<th>Versiunea în 10 (buster)</th>
<th>Versiunea în 11 (bullseye)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache</td>
<td>2.4.38</td>
<td>2.4.48</td>
</tr>
<tr>
<td>Serverul DNS BIND</td>
<td>9.11</td>
<td>9.16</td>
</tr>
<tr>
<td>Cryptsetup</td>
<td>2.1</td>
<td>2.3</td>
</tr>
<tr>
<td>Dovecot MTA</td>
<td>2.3.4</td>
<td>2.3.13</td>
</tr>
<tr>
<td>Emacs</td>
<td>26.1</td>
<td>27.1</td>
</tr>
<tr>
<td>Serverul implicit de postă electronică Exim</td>
<td>4.92</td>
<td>4.94</td>
</tr>
<tr>
<td>GNU Compiler Collection drepr compilor implicita</td>
<td>8.3</td>
<td>10.2</td>
</tr>
<tr>
<td>GIMP</td>
<td>2.10.8</td>
<td>2.10.22</td>
</tr>
<tr>
<td>GnuPG</td>
<td>2.2.12</td>
<td>2.2.27</td>
</tr>
<tr>
<td>Inkscape</td>
<td>0.92.4</td>
<td>1.0.2</td>
</tr>
<tr>
<td>biblioteca GNU C</td>
<td>2.28</td>
<td>2.31</td>
</tr>
<tr>
<td>lighttpd</td>
<td>1.4.53</td>
<td>1.4.59</td>
</tr>
<tr>
<td>Imagine de nucleu Linux</td>
<td>Seria 4.19</td>
<td>5.10 series</td>
</tr>
<tr>
<td>Ansamblul de unelte LLVM/-Clang</td>
<td>6.0.1 și 7.0.1 (implicit)</td>
<td>9.0.1 and 11.0.1 (default)</td>
</tr>
<tr>
<td>MariaDB</td>
<td>10.3</td>
<td>10.5</td>
</tr>
<tr>
<td>Nginx</td>
<td>1.14</td>
<td>1.18</td>
</tr>
<tr>
<td>OpenJDK</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>OpenSSH</td>
<td>7.9p1</td>
<td>8.4p1</td>
</tr>
<tr>
<td>Perl</td>
<td>5.28</td>
<td>5.32</td>
</tr>
<tr>
<td>PHP</td>
<td>7.3</td>
<td>7.4</td>
</tr>
<tr>
<td>Postfix MTA</td>
<td>3.4</td>
<td>3.5</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>11</td>
<td>13</td>
</tr>
<tr>
<td>Python 3</td>
<td>3.7.3</td>
<td>3.9.1</td>
</tr>
<tr>
<td>Rustc</td>
<td>1.41 (1.34 for armel)</td>
<td>1.48</td>
</tr>
<tr>
<td>Samba</td>
<td>4.9</td>
<td>4.13</td>
</tr>
<tr>
<td>Vim</td>
<td>8.1</td>
<td>8.2</td>
</tr>
</tbody>
</table>

### 2.2.2 Driverless scanning and printing

Both printing with CUPS and scanning with SANE are increasingly likely to be possible without the need for any driver (often non-free) specific to the model of the hardware, especially in the case of devices marketed in the past five years or so.

#### 2.2.2.1 CUPS and driverless printing

Modern printers connected by ethernet or wireless can already use driverless printing (https://wiki.debian.org/CUPSQuickPrintQueues), implemented via CUPS and cups-filters, as was described in the Release Notes for buster (https://www.debian.org/releases/buster/amd64/release-notes/ch-whats-new.html#driverless-printing). Debian 11 „bullseye“ brings the new package ipp-usb, which is recommended by cups-daemon and uses the vendor-neutral IPP-over-USB (https://wiki.debian.org/CUPSDriverlessPrinting#ipp-over-usb) protocol supported by many modern printers. This allows a USB device to be treated as a network device, extending driverless printing to include USB-connected printers. The specifics are outlined on the wiki (https://wiki.debian.org/CUPSDriverlessPrinting#ipp-usb).

The systemd service file included in the ipp-usb package starts the ipp-usb daemon when a USB-connected printer is plugged in, thus making it available to print to. By default cups-browsed should configure it automatically, or it can be manually set up with a local driverless print queue (https://wiki.debian.org/SystemPrinting).
2.2.2.2 SANE and driverless scanning

The official SANE driverless backend is provided by `sane-escl` in `libsane1`. An independently developed driverless backend is `sane-airscan`. Both backends understand the eSCL protocol (https://wiki.debian.org/SaneOverNetwork#escl) but `sane-airscan` can also use the WSD (https://wiki.debian.org/SaneOverNetwork#wsd) protocol. Users should consider having both backends on their systems. eSCL and WSD are network protocols. Consequently they will operate over a USB connection if the device is an IPP-over-USB device (see above). Note that `libsane1` has `ipp-usb` as a recommended package. This leads to a suitable device being automatically set up to use a driverless backend driver when it is connected to a USB port.

2.2.3 New generic open command

A new `open` command is available as a convenience alias to `xdg-open` (by default) or `run-mailcap`, managed by the `update-alternatives(1)` (https://manpages.debian.org//bullseye/dpkg/update-alternatives.1.html) system. It is intended for interactive use at the command line, to open files with their default application, which can be a graphical program when available.

2.2.4 Control groups v2

In bullseye, systemd defaults to using control groups v2 (cgroupv2), which provides a unified resource-control hierarchy. Kernel commandline parameters are available to re-enable the legacy cgroups if necessary; see the notes for OpenStack in Section 5.1.8 section.

2.2.5 Persistent systemd journal

Systemd in bullseye activates its persistent journal functionality by default, storing its files in `/var/log/journal/`. See `systemd-journald.service(8)` (https://manpages.debian.org//bullseye/systemd/systemd-journald.service.8.html) for details; note that on Debian the journal is readable for members of `adm`, in addition to the default `systemd-journal` group.

This should not interfere with any existing traditional logging daemon such as `rsyslog`, but users who are not relying on special features of such a daemon may wish to uninstall it and switch over to using only the journal.

2.2.6 New Fcitx 5 Input Method

Fcitx 5 is an input method for Chinese, Japanese, Korean and many other languages. It is the successor of the popular Fcitx 4 in buster. The new version supports Wayland and has better addon support. More information including the migration guide can be found on the wiki (https://wiki.debian.org/I18n/Fcitx5).

2.2.7 Noutăți de la Blend-ul Debian Med

The Debian Med team has been taking part in the fight against COVID-19 by packaging software for researching the virus on the sequence level and for fighting the pandemic with the tools used in epidemiology. The effort will be continued in the next release cycle with focus on machine learning tools that are used in both fields.

Besides the addition of new packages in the field of life sciences and medicine, more and more existing packages have gained Continuous Integration support.

A range of performance critical applications now benefit from SIMD Everywhere (https://wiki.debian.org/SIMDEverywhere). This library allows packages to be available on more hardware platforms supported by Debian (notably on arm64) while maintaining the performance benefit brought by processors supporting vector extensions, such as AVX on amd64, or NEON on arm64.

To install packages maintained by the Debian Med team, install the metapackages named `med-*`, which are at version 3.6.x for Debian bullseye. Feel free to visit the Debian Med tasks pages (https://blends.debian.org/med/tasks) to see the full range of biological and medical software available in Debian.
2.2.8 Kernel support for exFAT
bullseye is the first release providing a Linux kernel which has support for the exFAT filesystem, and defaults to using it for mounting exFAT filesystems. Consequently it’s no longer required to use the filesystem-in-userspace implementation provided via the `exfat-fuse` package. If you would like to continue to use the filesystem-in-userspace implementation, you need to invoke the `mount.exfat-fuse` helper directly when mounting an exFAT filesystem.

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

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

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

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

2.2.11 Initial availability of the Bazel build system
The Bazel build system (https://bazel.build/) is available in Debian starting with this release. This is a bootstrap variant that doesn’t include local versions of the extended Bazel ecosystem. However, the current package does provide identical functionality to core upstream Bazel, with the advantage of convenient Debian package management for the installation. While building Debian packages is not currently recommended yet, any software that supports Bazel builds should build normally using the `bazel-bootstrap` package. This includes build-time downloads of required dependencies.

The Debian Bazel Team (https://salsa.debian.org/bazel-team/meta) is working to package an extensible version of Bazel for future Debian releases. This extensible version will allow additional components of the Bazel ecosystem to be included as native Debian packages. More importantly, this version will allow Debian packages to be built using Bazel. Contributions to the team are welcome!
Capitolul 3

Sistemul de instalare

Programul de instalare Debian este sistemul de instalare oficial pentru Debian. Acesta oferă o varietate de metode de instalare. Metodele disponibile pentru instalarea sistemului depind de arhitectura sistemului dumneavoastră.

Imaginile programului de instalare pentru bullseye pot fi găsite împreună cu Ghidul de instalare pe situl Debian (https://www.debian.org/releases/bullseye/debian-installer/).

Ghidul de instalare mai este inclus și pe primul disc din seturile oficiale de DVD Debian (CD/blu-ray) la:
/doc/install/manual/<i>limbb''âb''</i>/index.html


3.1 Ce este nou în sistemul de instalare?

Programul de instalare Debian a avut parte de multe schimbări de la versiunea precedentă lansată oficial odată cu Debian 10, rezultând atât în suport mai bun pentru hardware cât și capacități noi, interesante.


3.1.1 Help with installation of firmware

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

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

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

3.1.2 Instalarea automată

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

Ghidul de instalare (https://www.debian.org/releases/bullseye/installmanual) conține acum o anexă separată și actualizată cu documentație amplă despre folosirea preconfigurărilor.
3.2 Container and Virtual Machine images

Multi-architecture Debian bullseye container images are available on Docker Hub (https://hub.docker.com/_/debian). In addition to the standard images, a “slim” variant is available that reduces disk usage.

Virtual machine images for the Hashicorp Vagrant VM manager are published to Vagrant Cloud (https://app.vagrantup.com/debian).
Capitolul 4

Actualizarea de la Debian 10 (buster)

4.1 Pregătirile pentru actualizare

Vă sugerăm ca înainte de actualizare să citiți informațiile din Cap. 5. Acel capitol tratează probleme potențiale care nu sunt legate direct de procesul de actualizare, dar care ar putea fi important de știut înainte să începeți.

4.1.1 Faceți copii de siguranță pentru orice date sau configurații

Înainte de a vă actualiza sistemul, este indicat să faceți o copie de siguranță completă, sau cel puțin a datelor sau a configurațiilor pe care nu vă permiteți să le pierdeți. Unelele și procesele de actualizare sunt foarte fiabile, însă o problemă hardware apărută în mijlocul actualizării poate afecta sever un sistem.

Cele mai importate lucruri de copiat sunt conținutul lui /etc, /var/lib/dpkg, /var/lib/apt/extended_states și rezultatul comenzi dpkg --get-sections "*" (ghilimelele sunt importante). Dacă folosiți aptitude pentru administrarea pachetelor de pe sistemul dumneavoastră veți trebui să salvați și /var/lib/aptitude/pkgstates.

Procesul de actualizare în sine nu modifică nicio în directorul /home. Totuși, unele aplicații (cum ar fi unele componente ale suitei Mozilla, mediile grafice GNOME și KDE) sunt cunoscute pentru faptul că suprascrivi valorile existente ale configurațiilor utilizatorilor cu noi valori implicite în momentul în care o versiune nouă a aplicației este pornită pentru prima oară de către utilizator. Ca măsură de precauție, veți dorbi probabil să faceți o copie de siguranță a fișierelor și directoarelor ascunse („.dotfiles” (n. trad. care încep cu punctul)) din directoarele utilizatorilor. Copia ar putea să vă ajute să restaurați sau să recreați vechile configurații. Probabil veți dorbi să informați și utilizatorii în acest sens.

Orice operație de instalare a pachetelor trebuie executată cu drepturi de superutilizator, deci fie vă autentificați ca root, fie utilizați su sau sudo pentru a obține drepturile de acces necesare. Operația de actualizare are câteva precondiții pe care va trebui să le verificați înainte de actualizare.

4.1.2 Informații utilizatorii din timp

Este o idee bună să informați din timp toți utilizatorii despre actualizările planificate, chiar dacă utilizatorii ce vă accezează sistemul prin conexiune ssh n-ar trebui să se siseze prea multe în timpul actualizării și ar trebui să-și poată continua lucrul.

Dacă doriti să vă luați măsuri suplimentare de precauție faceți o copie de siguranță sau demontați partitia /home înainte de actualizare.

Va trebui să faceți o înnoire de nucleu (n. trad. „kernel”) odată cu trecerea la bullseye, deci o repornire va fi necesară. În mod normal aceasta se face atunci când actualizarea este încheiată.

4.1.3 Pregătiri pentru indisponibilitatea serviciilor

Pot exista servicii oferite de sistem asociate cu pachete care vor fi incluse în actualizare. În acest caz țineți cont că aceste servicii vor fi opriți în timp ce pachetele asociate sunt înlocuite și configureate. În această perioadă, serviciile respective nu vor fi disponibile.
Timpul precis de indisponibilitate al acestor servicii variază în funcție de numărul de pachete actualizate în sistem și include de asemenea timpul necesar administratorului de sistem să răspundă la întrebările de configurare de la actualizările de pachete (dacă există). Țineți cont că, în cazul în care procesul de înnoire se face nesupravegheat și sistemul solicită informații pe parcursul actualizării, este foarte posibil ca serviciile să fie indisponibile pentru o perioadă de timp semnificativă.

Dacă sistemul de actualizat furnizează servicii critice pentru utilizatorii sau rețea, puteți reduce timpul de indisponibilitate dacă faceți o înnoire minimală, după cum este descrisă în Secțiune 4.4.4, urmată de o înnoire a nucleului și o repornire, iar apoi actualizați pachetele asociate cu serviciile critice. Actualizați aceste pachete înainte de actualizarea completă a sistemului descrisă în Secțiune 4.4.5. În acest fel puteți să vă asigurați că aceste servicii critice rulează și sunt disponibile pe durata întregului proces de înnoire, iar timpul în care sunt indisponibile este redus.

4.1.4 Pregătiri pentru recuperare

Deși Debian face tot posibilul ca sistemul să rămână capabil de pornire în orice moment există o șansă să întâmpinați probleme la reinițializarea sistemului după actualizare. Problemele potențiale cunoscute sunt documentate aici și în următorul capitol al acestor Note de lansare.

Din acest motiv are sens să vă asigurați că veți putea să recuperați sistemul în cazul în care acesta nu va mai reporni, sau va eșua la activarea rețelei, în cazul sistemelor la distanță.

Dacă faceti actualizarea de la distanță prin printr-o conexiune ssh este recomandabil să luați măsurile necesare pentru a putea accesa serverul printr-un terminal serial la distanță. Există posibilitatea ca după actualizarea nucleului și repornirea sistemului să fie nevoie să reparați configurația sistemului de la o consolă locală. De asemenea, dacă sistemul este repornit accidental în mijlocul actualizării există șansa să fie necesară recuperarea fososind o consolă locală.


If that fails, you will need an alternative way to boot your system so you can access and repair it. One option is to use a special rescue or live install (https://www.debian.org/CD/live/) image. After booting from that, you should be able to mount your root file system and chroot into it to investigate and fix the problem.

4.1.4.1 Consolă de depanare în timpul inițializării fososind inîntrd

Pachetul initramfs-tools include un interpreter de comenzi miniati în imaginile inîntrd pe care le generează. De exemplu, dacă imaginea inîntrd nu poate să monteze sistemul de fișiere rădăcină, veți fi transferat la acest interpretor de comenzi, care dispune de comenzi de bază pentru a putea detecta și eventual rezolva problema.

Lucruri uzuale pe care ar trebui să le verificați: prezența fișierelor-dispozitiv corecte în /dev; ce module sunt încărcate (cat /proc/modules); rezultatul comenzi dmesg, pentru erori la încărcarea driverelor. Rezultatul comenzi dmesg va arăta și care fișier-dispozitiv au fost alocate discurilor. Ar trebui să comparați cu rezultatul comenzi echo $ROOT pentru a vă asigura că sistemul de fișiere rădăcină este pe dispozitivului la care vă așteptați.

Dacă reușiți să corectați problema puteți ieși din consola de depanare cu comanda exit, iar apoi se va continua procesul de inițializare de la punctul în care a eșuat. Desigur, va trebui să reparați problema la bază și să regenerați imaginea inîntrd pentru ca următoarea inițializare să nu eșueze din nou.

1Dacă prioritatea deboconf este stabilată la un nivel foarte ridicat puteți preveni întrebările de configurare, dar serviciile care se bazează pe opțiuni de configurare implicite care nu se aplică sistemului dumneavoastră nu vor porni.

2Spre exemplu: serviciile DNS sau DHCP, mai ales dacă nu există redundanță sau soluție de înlocuire. În cazul DHCP utilizatorii pot fi deconectați de la rețea dacă timpul de alocare al adresei este mai mic decât timpul necesar procesului de actualizare.

3Această facilitate poate fi dezactivată prin adăugarea parametrului panic=0 la parametrii de inițializare.
4.1.4.2 Consola de depanare în timpul inițializării folosind systemd

Dacă inițializarea eșuează rulând systemd este posibil să obțineți o consolă de depanare root (cu drepturi de administrator) modificând linia de comandă a nucleului. Dacă inițializarea reușește, dar unele servicii nu pornesc, ar putea fi utilizat sistemd.unit=rescue.target la parametrul nucleului.

Altfel, parametrul de nucleu systemd.unit=emergency.target va oferi o consolă de administrare cât se poate de repede. Totuși, aceasta se va întâmplă înainte de montarea sistemului de fișiere rădăcină cu permisiuni citire-scriere. Va trebui să faceți asta manual cu:

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

Mai multe informații despre depanarea unei inițializări cu systemd nefuncționale pot fi găsite în articolul Diagnosticarea problemelor de inițializare a sistemului (http://freedesktop.org/wiki/Software/systemd/Debugging/).

4.1.5 Pregătiți un mediu sigur pentru actualizare

**IMPORTANT**

Dacă utilizați servicii VPN (cum ar fi tinc) este posibil ca acestea să nu fie disponibile pe tot parcursul procesului de actualizare. Mai multe informații la Secțiune 4.1.3.

Pentru a avea o marjă de siguranță suplimentară atunci când actualizați de la distanță vă sugerăm să rulați procesul de actualizare într-o consolă virtuală furnizată de programul screen. Acesta permite reconectarea în siguranță iar procesul de actualizare nu este întrerupt, chiar dacă procesul conexiunii la distanță eșuează temporar.

4.2 Start from „pure” Debian

The upgrade process described in this chapter has been designed for „pure” Debian stable systems. APT controls what is installed on your system. If your APT configuration mentions additional sources besides buster, or if you have installed packages from other releases or from third parties, then to ensure a reliable upgrade process you may wish to begin by removing these complicating factors.

Fișierul principal de configurare folosit de APT pentru a decide de la ce surse va descărca pachete este /etc/apt/sources.list, dar poate folosi și fișiere din directorul /etc/apt/sources.list.d/ pentru detalii vedere sources.list(5) (https://manpages.debian.org/bullseye/apt/sources.list.5.html). Dacă sistemul dumneavoastră folosește fișiere source-list multiple trebuie să vă asigurați că sunt consevenge.

4.2.1 Upgrade to Debian 10 (buster)

Direct upgrades from Debian releases older than 10 (buster) are not supported. Display your Debian version with:

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

Please follow the instructions in the Release Notes for Debian 10 (https://www.debian.org/releases/buster/releasenotes) to upgrade to Debian 10 first.

4.2.2 Remove non-Debian packages

Mai jos sunt două metode pentru a găsi pachete instalate care nu provin de la Debian, folosind aptitude sau apt-forktracer. Rețineți că niciuna din metode nu are acuratețe 100% (exemplul cu aptitude va lista pachete furnizate în trecut de Debian, cum ar fi pachete vechi de nucleu).
4.2.3 Upgrade to latest point release

This procedure assumes your system has been updated to the latest point release of buster. If you have not done this or are unsure, follow the instructions in Section A.1.

4.2.4 Prepare the package database

You should make sure the package database is ready before proceeding with the upgrade. If you are a user of another package manager like aptitude or synaptic, review any pending actions. A package scheduled for installation or removal might interfere with the upgrade procedure. Note that correcting this is only possible if your APT source-list files still point to buster and not to stable or bullseye; see Section A.2.

4.2.5 Remove obsolete packages

It is a good idea to remove obsolete packages from your system before upgrading. They may introduce complications during the upgrade process, and can present security risks as they are no longer maintained.

4.2.6 Clean up leftover configuration files

A previous upgrade may have left unused copies of configuration files; old versions of configuration files, versions supplied by the package maintainers, etc. Removing leftover files from previous upgrades can avoid confusion. Find such leftover files with:

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

4.2.7 The security section

For APT source lines referencing the security archive, the format has changed slightly along with the release name, going from buster/updates to bullseye-security; see Secțiune 5.1.2.

4.2.8 Secțiunea proposed-updates

Dacă aveți secțiunea proposed-updates (n. trad. actualizări propuse) în fișierele source-list ale APT ar fi bine să o ștergeți înainte de a încerca să actualizați sistemul. Aceasta este o precauție pentru a reduce probabilitatea unor conflicte.

4.2.9 Surse neoficiale

Dacă aveți pachete non-Debian pe sistemul dumneavoastră ar trebui să știți că acestea ar putea fi șterse în cursul actualizării datorită unor conflicte de dependențe. Dacă aceste pachete au fost instalate prin adăugarea unei arhive suplimentare în fișierele source-list ale APT ar trebui să verificați dacă această arhi ă oferă pachete compilate pentru bullseye și să schimbați sursa corespunzătoare la același moment cu schimbarea surselor pentru pachetele Debian.

Unii utilizatori ar putea avea instalate pe sistemele lor buster versiuni neofici ale tip backport „mai noi” ale unor pachete care sunt în Debian. Aceste pachete pot cauza probleme în timpul unei actualizări deoarece pot rezulta în conflicte de fișiere⁴. Secțiune 4.5 conține informații despre cum să rezolvați conflictele de fișiere dacă apar.

⁴În mod normal sistemul de management al pachetelor din Debian nu permite unui pachet să șteargă sau să înlocuiască un fișier deținut de alt pachet, decât în cazul în care a fost definit ca înlocuitor pentru acel pachet.
4.2.10 Dezactivarea alegerilor selective APT

If you have configured APT to install certain packages from a distribution other than stable (e.g. from testing), you may have to change your APT pinning configuration (stored in /etc/apt/preferences and /etc/apt/preferences.d/) to allow the upgrade of packages to the versions in the new stable release. Further information on APT pinning can be found in apt_preferences(5) (https://manpages.debian.org/bullseye/apt/apt_preferences.5.en.html).

4.2.11 Check package status

Indiferent de metoda utilizată pentru actualizare, se recomandă să verificați mai întâi starea tuturor pachetelor și să vă asigurați că toate pachetele sunt într-o stare actualizabilă. Următoarea comandă vă afișează evenualele pachete care au starea de Half-Installed (n. trad. jumătate-instalat) sau Failed-Config (n. trad. eșec-configurare), precum și cele cu o stare de eroare.

```
# dpkg --audit
```

Ați putea să inspectați starea tuturor pachetelor de pe sistemul dumneavoastră și utilizând aptitude sau folosind comenzii precum

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

sau

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

Este preferabil să ștergeți orice marcă „păstrat” (n. trad. „hold”) înainte de actualizare. Actualizarea va eșua dacă este păstrat un pachet esențial pentru actualizare.

De reținut că aptitude folosește o metodă diferită de a marca pachetele care sunt păstrate față de apt și dselect. Puteti identifica pachetele păstrate de aptitude cu

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

Dacă vreți să verificați ce pachete aveți păstrate de apt folosiți

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

Dacă ați modificat și recompilat local un pachet și nu l-ați redenumit sau nu ați adăugat o „epocă” la versiune, va trebui să îl „păstrați” pentru a nu fi actualizat.

Starea „hold” pentru apt poate fi schimbată folosind:

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

Înlocuiți hold cu install pentru a șterge starea „hold”.

Dacă mai aveți ceva de rezolvat este cel mai bine vă asigurați că fișierele source-list APT încă fac referire la buster, după cum este explicat în Section A.2.

4.3 Pregătirea surselor pentru APT

Before starting the upgrade you must reconfigure APT source-list files (/etc/apt/sources.list and files under /etc/apt/sources.list.d/) to add sources for bullseye and typically to remove sources for buster.

APT va lua în considerare toate pachetele care pot fi găsite prin intermediul oricărei arhive de pachete configureate și va instala pachetul cu cea mai mare versiune, alegând prioritar prima linie din fișiere. În cazul în care aveți mai multe locații cu pachete ar trebui să listați în primul rând cele de pe discuri locale, după care CD-uri, iar după aceea cele de la distanță.

O versiune poate fi menționată atât prin numele de cod (de ex: buster, bullseye) cât și prin numele de stare (ex: oldstable, stable, testing, unstable). Referirea la o versiune folosind numele de cod are avantajul că nu veți fi luat prin surprindere de o nouă versiune, motiv pentru care am folosit această abordare aici. Evident, aceasta înseamnă că va trebui să urmăriți anunțurile de lansare.

Dacă utilizați numele de stare veți observa multe actualizări pentru pachete, disponibile imediat ce o versiune a fost lansată.

Debian pune la dispoziție două liste de e-mail cu anunțuri care vă ajută să rămâneți la curent cu informațiile relevante despre lansările Debian:
4.3.1 Adăugarea de surse internet pentru APT

La instalări noi implicit APT este configurat să folosească serviciul Debian APT CDN (n. trad. CDN - „Content Delivery Network”, rețea de distribuție de conținut). În felul acesta pachetele ar trebui să fie descărcate automat de la un server apropiat în rețea. Deoarece acesta este un serviciu nou instalările mai vechi ar putea fi configureate să preia pachete de la serverele principale Debian sau unul din siturile oglindă. Este recomandat să comutați la utilizarea serviciului CDN în configurația APT, în cazul în care nu ați făcut deja acest lucru.

Pentru a utiliza serviciul CDN adăugați o linie ca aceasta în configurația APT (se presupune că folosiți secțiunile main și contrib):

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

După ce adăugați noile surse dezactivați liniile „deb” care existau înainte, prin introducerea unui diez (#) la începutul lor.

Totuși, dacă obțineți rezultate mai bune folosind un site-oglindă specific care este mai apropiat din punct de vedere al rețelei, această opțiune este disponibilă în continuare.

Adresele siturilor-oglindă Debian pot fi găsite la [https://www.debian.org/distrib/ftplist](https://www.debian.org/distrib/ftplist) (vedeți secțiunea „lista serverelor Debian”).

De exemplu, să presupunem că cel mai apropiat sit-oglindă Debian este [http://mirrors.kernel.org](http://mirrors.kernel.org). Dacă inspectați această locație cu un navigator web, veți observa că directoarele principale sunt organizate astfel:

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

Pentru a configura APT să folosească un sit-oglindă, adăugați o linie ca aceasta (se presupune din nou că folosiți main și contrib):

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

Observații: ”dists” este adăugat implicit, iar argumentele de după numele versiunii sunt utilizate pentru a extinde calea în directoare multiple.

Din nou, după ce adăugați sursele noi, dezactivați înregistrările pentru arhive existente anterior.

4.3.2 Adăugarea de surse APT pentru un sit-oglindă local

În loc să folosiți situri-oglindă poate doriți să modificați fișierele source-list APT pentru a folosi o sursă de pe un disc local (eventual montat prin NFS).

De exemplu, locația dumneavoastră cu pachete poate fi în `/var/local/debian/`, având directoarele principale astfel:

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

Pentru a utiliza această locație cu `apt` adăugați această linie în fișierul `sources.list`:

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

Observații: ”dists” este adăugat implicit, iar argumentele de după numele versiunii sunt utilizate pentru a extinde calea în directoare multiple.

După ce ați adăugat noile surse dezactivați liniile pentru arhive care existau deja în fișierele source-list ale APT prin plasarea unui diez (+) la începutul lor.
4.3.3 Adăugarea de surse APT de pe un mediu optic

Dacă doriți să folosiți doar DVD-uri (sau CD-uri sau discuri Blu-ray), dezactivați liniile existente din fișierele source-list APT, prin plasarea unui diez (#) la începutul lor.

Asigurați-vă că există o linie în /etc/fstab ce permite montarea CD-ROM-ului la locația /media/cdrom. De exemplu, dacă unitatea CD-ROM este /dev/sr0 atunci /etc/fstab ar trebui să conțină o linie de genul:

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

De reținut că între cuvintele noauto, ro din cel de-al patrulea câmp nu trebuie să existe niciun spațiu.

Pentru a verifica introduceți un CD și încercați să rulați

```
# mount /cdrom  # monteazăb’’ăb’’ CD-ul în punctul de montare
# ls -a/lF /cdrom # afib’d’b’eazb’’ăb’’ directorul rb’’ăb’’db’’ăb’’cinb’’ăb’’ ← din CD
# umount /cdrom  # demonteazăb’’ăb’’ CD-ul
```

Apoi rulați

```
# apt-cdrom add
```

pentru fiecare CD-ROM Debian cu binare pe care îl aveți, pentru a adăuga datele despre fiecare CD în baza de date APT.

4.4 Actualizarea pachetelor

Metoda recomandată de actualizare de la versiuni anterioare Debian este să folosiți utilitarul de gestionare a pachetelor apt.

**NOTĂ**

Comanda **apt** este destinată folosirii interactive și nu ar trebui folosită în scripturi. În scripturi ar trebui folosită comanda **apt-get**, care produce răspunsuri stabilă, mai potrivite pentru procesare automată.

Nu uitați să montați toate particițiile necesare (în special partitura rădăcină și partitia /usr) în mod citire-scriere, cu o comandă ca:

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

În continuare ar trebui să verificați că sursele APT (din /etc/apt/sources.list și fișierele din /etc/apt/sources.list.d/) fac referință la „bullseye” sau la „stable”. Nu ar trebui să fie nicio sursă care se referă la buster.

**NOTĂ**

Liniile de surse pentru CD-uri pot conține uneori „unstable”. Deși acest lucru poate fi deruantul ele **nu** trebuie schimbate.

4.4.1 Înregistrarea sesiunii

Este recomandat să utilizați programul **/usr/bin/script** pentru a înregistra sesiunea de actualizare. În cazul în care intervine vreo problemă veți avea un istoric a ceea ce s-a întâmplat, iar dacă este nevoie, veți putea oferi informații exacte când raportați problema. Pentru a porni înregistrarea, tastați:
CAPITOLUL 4. ACTUALIZAREA DE LA DEBIAN ...

4.4. ACTUALIZAREA PACHETELOR

sau similar. Dacă trebuie să porniți înregistrarea din nou (ex. dacă trebuie să reporniți sistemul) folosiți valori diferite pentru etapă pentru a indica ce etapă a actualizării este înregistrată. Nu puneti fișierul script într-un director temporar cum ar fi /tmp sau /var/tmp (fișiere în aceste directoare ar putea fi șterse în timpul actualizării sau la o repornire).

Înregistrarea vă va permite, de asemenea, să consultați informații care au derulat în afara ecranului. Dacă sunteți consola sistemului puteți trece la VT2 (folosind Alt-F2) și după autentificare să utilizați less -R ~root/actualizare-bullseye.script pentru a vedea fișierul.

După încheierea actualizării, puteți opri comanda script tastând exit la prompt.


Dacă ați folosit opțiunea -t pentru script puteți folosi programul scriptreplay pentru a reda întreaga sesiune:

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

4.4.2 Actualizarea liste de pachete

Mai întâi trebuie preluată lista pachetelor disponibile în noua versiune. Aceasta se face cu:

```
# apt update
```

NOTĂ

Utilizatorii care folosesc apt-secure ar putea avea probleme cu aptitude sau apt-get. Pentru apt-get puteți folosi apt-get update --allow-releaseinfo-change.

4.4.3 Verificați dacă aveți suficient spațiu pentru actualizare

Înainte de a începe actualizarea completă descrisă în Secțiune 4.4.5 va trebui să vă asigurați că aveți suficient spațiu pe disc. În primul rând, orice pachet necesar pentru instalare descărcat prin rețea este stocat în /var/cache/apt/archives (și subdirectorul partial/ în timpul descărcării), deci trebuie să aveți suficient spațiu pe sistemul de fișiere pe care se află /var/ pentru a descărca pachetele ce vor fi instalate pe sistemul dumneavoastră. După descărcare veți avea nevoie de mai mult spațiu pe alte partiții de sistem pentru a instala atât pachetele actualizate (care e posibil să conțină binare mai mari sau mai multe date) cât și pachetele noi care vor fi aduse pentru actualizare. Dacă sistemul dumneavoastră nu are suficient spațiu este posibil să rămâneți cu o actualizare incompletă, care este foarte dificil de recuperat.

apt vă poate arăta informații detaliate despre spațiu necesar pentru instalare. Înainte să începeți actualizarea, puteți vedea această estimare folosind comanda:

```
# apt -o APT::Get::Trivial-Only=true full-upgrade
[ ... ]
XXX actualizate, XXX noi instalate, XXX de indep."'ab'"rtat b'"sb'"i XXX ←
neactualizate.
Trebuie desc'b'"sb'"crate xx.xMB de archive.
Dup'b'"sb'" aceastb'"sb'" operab'"tb'"iune, AAAAMB spab'"tb'"iu suplimentar va fi ←
folosit.
```

16
NOTĂ
Această comandă ar putea genera o eroare la începutul procedeului de actualizare din motive descrise în următoarele secțiuni. În acest caz va trebui să așteptați până ați făcut o actualizare minimală conform Secțiune 4.4.4 înainte de a rula această comandă pentru a estima spațiul pe disc.

Dacă nu aveți spațiu suficient pentru actualizare, apt vă va avertiza cu un mesaj așa cum urmează:

E: Nu aveb’’tb’’i spab’’tb’’iu liber suficient în /var/cache/apt/archives/.

În această situație eliberăți spațiu înainte de actualizare. Aveți mai multe opțiuni:

- Ștergeți pachetele care au fost descărcate anterior pentru a fi instalate (în /var/cache/apt/archive). Curățarea depozitului temporar de pachete se face cu comanda apt clean, care va șterge toate fișierele descărcate anterior.

- Îndepărtați pachetele uitate. Dacă ați utilizat aptitude sau apt pentru a instala manual pachete în buster, aceasta vor reține faptul că au fost instalate manual și vor putea marca drept inutil pachetele care au fost instalate doar ca dependențe și nu mai sunt necesare deoarece pachetele care aveau nevoie de ele au fost șterse. În consecință nu vor marca pentru ștergere pachetele pe care le-ați instalat manual. Pentru a îndepărta pachetele instalate automat și care nu mai sunt folosite, executați:

```bash
apt autoremove
```

Puteți folosi și deborphan, debfoster sau cruft pentru a găsi pachetele inutilizate. Nu dezinstalați pachetele prezentate de aceste unelte fără o examinare atentă, mai ales dacă folosiți opțiunile agresive, neimplicite, care sunt susceptibile de a da rezultate eronate cu privire la starea pachetelor. Este indicat să analizați manual pachetele sugerate pentru dezinstalare (ex: conținutul, dimensiunea și descrierea) înainte de a le dezinstala.


- Ștergeți fișierele de traducere și localizare din sistem în caz că nu mai sunt necesare. Puteți instala și configura pachetul localepurge astfel încât doar câteva localizări selectate să fie păstrate. Astfel se va reduce din spațiul ocupat în /usr/share/locale.

- Mutați temporar pe un alt sistem sau ștergeți permanenți fișierele jurnal de sistem din /var/log/.

- Folosiți un /var/cache/apt/archives temporar: pentru depozitul temporar puteți folosi un director de pe un alt sistem de fișiere (dispozitiv de stocare USB, disc instalat temporar, un alt sistem de fișiere în utilizare, ...).

NOTĂ
Nu folosiți o partitură NFS deoarece conexiunea la rețea ar putea fi întreruptă în timpul actualizării.
De exemplu, dacă aveți un dispozitiv USB montat la `/media/stick-usb`:

1. ștergeți pachetele care au fost descărcate anterior spre instalare:
   
   ```
   # apt clean
   ```

2. copiați directorul `/var/cache/apt/archives` pe dispozitivul USB:
   
   ```
   # cp -ax /var/cache/apt/archives /media/stick-usb/
   ```

3. montați directorul pentru depozit temporar peste cel curent:
   
   ```
   # mount --bind /media/stick-usb/archives /var/cache/apt/archives
   ```

4. după actualizare restaurați directorul `/var/cache/apt/archives original`:
   
   ```
   # umount /media/stick-usb/archives
   ```

5. ștergeți directorul `/media/stick-usb/archives`.

Puteți crea directorul pentru depozit temporar pe orice sistem de fișiere montat pe sistemul dumneavoastră.

- Executați o actualizare minimală a sistemului (cititi Secțiune 4.4.4) sau actualizări parțiale a sistemului urmată de o actualizare completă. Acest lucru va face posibil să actualizați sistemul parțial și va permite curățarea depozitului temporar de pachete înainte de actualizarea completă.

Țineți cont că pentru a putea șterge pachete în siguranță se recomandă să treceți fișierele source-list ale APT înapoi la buster după cum este descris în Section A.2.

### 4.4.4 Actualizare de sistem minimală

**IMPORTANT**

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

În unele cazuri, o actualizare completă (așa cum este descrisă mai jos), ar putea șterge un număr mare de pachete pe care dorïți să le păstrați. În acest caz vă recomandăm o actualizare în doi pași: mai întâi o actualizare minimală pentru a depăși aceste conflictele, după aceea o actualizare completă așa cum este descrisă în Secțiune 4.4.5.

Pentru a face acest lucru mai întâi rulați:

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

Aceasta are ca efect actualizarea acelor pachete care pot fi actualizate fără ca altele pachete să fie șterse, dar va instala pachete noi dacă este necesar.

Actualizarea minimală a sistemului poate fi folosită și atunci când sistemul nu dispune de spațiu suficient și nu se poate face o actualizare completă datorită constrângerilor de spațiu. Dacă pachetul `apt-listchanges` este instalat acesta va afișa informații importante despre pachetele actualizate (în configurația implicită) după descărcarea pachetelor. Pentru a ieși din programul de afișare și a continua actualizarea apăsați `q` după ce ați citit.

### 4.4.5 Actualizarea sistemului

Dacă ați executat pașii anterioiri puteți continua cu partea principală a actualizării. Execuți:

```
# apt full-upgrade
```
Aceasta va efectua o actualizare completă a sistemului, instalând cele mai noi versiuni disponibile ale tuturor pachetelor și va rezolva toate posibilele schimbări de dependențe dintre pachetele din diferitele versiuni. Dacă este necesar va instala câteva pachete noi (de obicei versiuni de biblioteci mai noi sau pachete redenumite) și va șterge pachetele învăchite care intră în conflict cu cele noi.

Când actualizați de pe un set de CD/DVD/BD-uri, vi se va cere să introduceți anumite discuri la diverse momente în timpul actualizării. Este posibil să trebuiască să introduceți de mai multe ori același disc. Acest lucru este necesar datorită pachetelor interdependente dispărute pe mai multe discuri.

Pachetele deja instalate care nu pot fi înnoite la versiuni mai noi fără a schimba starea de instalare a unui alt pachet vor fi lăsatate la versiunea curentă (marcate ca „held back”). Acest lucru poate fi rezolvat prin utilizarea comenzii aptitude și alegerea acestor pachete pentru instalare sau prin rularea comenzii apt install pachet.

### 4.5 Probleme posibile în timpul actualizării

Secțiunile următoare descriu probleme cunoscute care pot apărea în timpul procedeului de actualizare la bullseye.

#### 4.5.1 Dist-upgrade eșuează cu eroarea „Could not perform immediate configuration”

În anumite cazuri etapa apt full-upgrade poate să eșueze după descărcarea pachetelor cu:

```text
E: Nu s-a putut face configurarea imediata: 'ab' cu 'i<nume_pacakage>/i'. Vb' -> 'ab' rugb'ab'm citib''tb' i in pagina de manual man 5 apt.conf secb''tb' -> iunea APT::Immediate-Configure pentru detalii.
```

Dacă se întâmplă acest lucru, rularea comenzii apt full-upgrade -o APT::Immediate-Configure = 0 ar trebui să permită continuarea actualizării.

O altă posibilă ocolire a problemei ar fi să adăugați temporar surse APT pentru buster și bullseye în sources.list și să rulați apt update.

#### 4.5.2 Pachet de îndepărtat

Procesul de actualizare la bullseye ar putea solicita îndepărtarea unor pachete din sistem. Lista exactă de pachete va fi diferită în funcție de setul de pachete pe care le aveți instalate. Aceste note de lansare oferă sfaturi generice despre programele care vor fi îndepărtate, dar dacă aveți îndoioși, este recomandată examinarea listei cu pachete propuse pentru a fi șterse de fiecare metodă de instalare, înainte de a continua. Pentru mai multe informații despre pachetele învăchite în bullseye, vizitați Secțiunea 4.8.

#### 4.5.3 Conflicte sau cicluri de pre-dependențe

Uneori este necesar să activați opțiunea APT::Force-LoopBreak în APT pentru a putea elimina temporar un pachet esențial, datorită unei bucle Conflict/Pre-Depenendență. apt vă va avertiza în legătură cu aceasta și va abandona actualizarea. Puteți ocolii această situație precizând opțiunea --o APT::Force-LoopBreak=1 în linia de comandă pentru apt.

Este posibil ca structura dependențelor dintr-un sistem să fie coruptă într-o asemenea măsură încât să necesite intervenție manuală. În mod obișnuit aceasta înseamnă utilizarea apt sau

```bash
# dpkg --remove nume_pachet
```

pentru a elimina pachetele problemă, sau

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

În cazuri extreme ar putea fi nevoie să forțați o reinstallare cu comanda

```bash
# dpkg --install <i>/cale/cb''ab''tre/nume_pachet.deb</i>
```
4.5.4 Conflict de fișiere

Dacă actualizați de la un sistem buster „pur” nu ar trebui să apară conflicte de fișiere, însă acestea pot interveni dacă aveți pachete neoficiale de tip „backport”. Un conflict de fișiere poate rezulta într-un eroare de genul:

```
Se despacheteazb''ăb'' <li><pachet-foo</li>(din <li><pachet-foo-fib''şb''ier</li>/i → <i>... dpkg: eroare la procesarea <li><pachet-foo</li>(--install):
  se încercă''ăb'' suprascripte arii <li><ceva-nume-fib''şb''ier</li>/i',
care este ''şb''i în pachetul <li><pachet-bar</li>/i>
dpkg-deb: subprocess paste killed by signal (Broken pipe)
Au fost întâmpinate erori în timpul procesb''ăb''rii:
<li><pachet-foo</li>/i>
```

Puteți încerca să rezolvați un conflict de fișiere prin eliminarea forțată a pachetelor menționate în ultima linie a mesajului de eroare:

```
# dpkg -r --force-depends nume_pachet
```

După ce ați rezolvat problema, ar trebui să puteți continua actualizarea prin repetarea comenzilor apt descrise mai sus.

4.5.5 Modificări ale configurațiilor

În timpul actualizării vor apărea întrebări referitor la configurarea sau re-configurarea mai multor pachete. Dacă sunteți întrebat dacă un fișier din directorul /etc/init.d sau fișierul /etc/manpath.config ar trebui înlocuit cu versiunea responsabilului de pachet, în general este necesar să răspundeți cu „da” (“yes” în engleză) pentru a asigura integritatea sistemului. Puteți oricând reveni la versiunile vechi, deoarece acestea vor fi salvate cu extensia .dpkg-old.

Dacă nu știți sigur ce să faceți, scrieți numele pachetului sau fișierului și amânați rezolvarea problemelor pentru mai târziu. Puteți căuta în fișierul script informația afișată în timpul actualizării.

4.5.6 Schimbare a sesiunii la consolă

Dacă faceți actualizarea folosind consola de sistem locală este posibil ca la un moment dat în timpul actualizării consola să fie mutată într-o altă vizualizare iar procesul de actualizare să nu mai fie vizibil. Acest lucru se poate întâmpina spre exemplu pe sisteme cu interfață grafică când este repornit managerul de display.

Pentru a recupera consola cu procesul de actualizare în derulare va trebui să folosiți Ctrl + Alt + F1 (dacă sunteți în mediul grafic) sau Alt + F1 (dacă sunteți în modul text) pentru a vă înțelege la terminalul virtual 1. Înlocuiți F1 cu tasta funcțională cu același număr ca terminalul virtual pe care se derulează procesul de actualizare. Puteți de asemenea să folosiți Alt + săgeată-stânga sau Alt + săgeată-dreapta pentru a schimba între diferitele terminale în mod text.

4.6 Actualizarea nucleului și a pachetelor conexe

Această secțiune explică actualizarea nucleului (n. trad. „kernel”) și identifică potențialele probleme legate de aceasta. Puteți instala unul din pachetele linux-image-* oferite de Debian sau să compilați un nucleul personalizat din surse.

O mare parte din informația expusă în această secțiune presupune că veți folosi un nucleu modular din Debian împreună cu initramfs-tools și udev. Dacă ați ales să folosiți un nucleu ce nu necesită întrid cu este folosit un alt generator de întrid atunci o parte din aceste informații ar putea să nu fie relevante.

4.6.1 Instalarea meta-pachetului de nucleu

Dacă nu ați făcut deja acest lucru, este indicat să instalați un meta-pachet linux-image-* atunci când efectuați actualizarea completă (n. trad. „full-upgrade”) de la buster la bullseye. Acest pachet vor aduce automat o nouă versiune de nucleu în timpul actualizărilor. Puteți verifica dacă aveți instalat un asemenea pachet cu comanda:
4.7 Pregătirile pentru următoarea versiune

După actualizare sunt anunțate pregătiri pe care le puteți face pentru următoarea lansare.

- Îndepărtarea pachetei înutile sau învechite după cum este descris în Secțiune 4.4.3. Ar trebui să verificați ce fișiere de configurare sunt folosite de aceasta și să luați în considerare eliminarea pachetelor (n. trad. „purge”) pentru a îndepărta fișierele de configurare. Vedeți și Secțiune 4.7.1.

4.7.1 Eliminarea pachetelor îndepărtate

În general este recomandat să eliminați complet pachetele îndepărtate, mai ales dacă acestea au fost îndepărtate în urma unei actualizări anterioare (de exemplu actualizarea la buster) sau erau furnizate de tești. În special scripturile vechi de tip init.d ar putea cauza probleme.

**ATENȚIE**

Eliminarea unui pachet va curăța în general și fișierele jurnal ale acestuia, poate doriți să salvați o copie înainte.

Comanda următoare afișează o listă cu toate pachetele îndepărtate care încă pot avea fișiere de configurare pe sistem:

```
# dpkg -l | awk ‘/\^rc/ { print $2 }’
```

Pachetele pot fi curățate folosind comanda `apt purge`. Dacă doriți să ștergeți toate pachetele odată, puteți folosi următoarea comandă:

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

Dacă folosiți `aptitude` puteți folosi și următoarea comandă alternativă:

```
# aptitude search ‘~c’
# aptitude purge ‘~c’
```

ATENȚIE: Eliminarea unui pachet va curăța în general și fișierele jurnal ale acestuia, poate doriți să salvați o copie înainte.
4.8 Pachete învechite

Deși aduce multe pachete noi, bullseye mai retrade și omite un număr de pachete vechi care au fost în buster. Nu se oferă nicio modalitate de tranziție pentru aceste pachete. Deși nimic nu vă oprește să continuați să folosiți un pachet învechit, proiectul Debian va opri suportul de securitate pentru ele la un an după lansarea lui bullseye și nu va oferi alt suport între timp. Se recomandă înlocuirea lor cu alternative, dacă acestea există.

Există multe motive pentru care pachetele pot fi scoase din distribuție: nu mai sunt întreținute de către autori originari, nu mai există un dezvoltator Debian interesat de întreținerea pachetelor, funcționalitatea oferită a fost înlocuită de alt software (sau o nouă versiune), sau nu mai sunt considerate a fi adecvate pentru bullseye datorită unor probleme. În cazul din urmă, pachetele ar putea fi încă prezentă în distribuția „unstable” (n. trad. „instabilă”).

Anumite interfețe pentru managementul pachetelor oferă modalități simple de a găsi pachete care nu mai sunt disponibile din sursele cunoscute. Interfața în mod text aptitude le afișează în categoria „Obsolete and Locally Created Packages” (n. trad. Pachete învechite și create local). Aceste pot fi afișate și eliminate din linia de comandă cu:

```
# aptitude search ‘~o’
# aptitude purge ‘~o’
```


Pentru o listă cu pachete învechite în Bullseye, vizitați Secțiune 5.3.1.

4.8.1 Pachete de tranziție

Există posibilitatea ca unele pachete din buster să fie înlocuite în bullseye cu pachete de tranziție „dummy” (n. trad. marionetă), care sunt pachete goale pentru simplificarea actualizării. Spre exemplu, dacă o aplicație care era distribuită într-un singur pachet a fost împărțită în mai multe pachete, este posibil să fie furnizat un pachet de tranziție cu același nume ca al pachetului vechi și cu dependențele astfel încât pachetele noii să fie instalate. După instalare, pachetul de tranziție fi îndepărtat fără probleme.

De obicei descrierile pachetelor de tranziție indică scopul lor, dar acestea nu sunt uniforme. În special unele pachete „dummy” sunt concepute pentru a fi păstrate, pentru instalarea unei suite software complete sau pentru a instala cea mai nouă versiune a unui program. Comanda deborphan cu opțiunile `--guess-*` (de ex. `--guess-dummy`) este utilă pentru a detecta pachete de tranziție.

---

5Sau atât timp cât nu se lanseză o altă versiune în acel interval de timp. În mod obișnuit doar două versiuni stable sunt suportate în același timp.
Capitolul 5

Probleme în bullseye de care ar trebui să știți


5.1 Elemente specifice actualizării la bullseye

Această secțiune tratează elemente legate de actualizarea de la buster la bullseye.

5.1.1 The XFS file system no longer supports barrier/nobarrier option

Support for the barrier and nobarrier mount options has been removed from the XFS file system. It is recommended to check /etc/fstab for the presence of either keyword and remove it. Partitions using these options will fail to mount.

5.1.2 Changed security archive layout

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

The security line in your APT configuration may look like:

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

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

APT::Default-Release "bullseye(\|security\|updates)$";

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

5.1.3 Password hashing uses yescrypt by default

The default password hash for local system accounts has been changed from SHA-512 to yescrypt. This is expected to provide improved security against dictionary-based password guessing attacks, in terms of both the space and time complexity of the attack.

To take advantage of this improved security, change local passwords; for example use the passwd command.

Old passwords will continue to work using whatever password hash was used to create them.
5.1. Elements specific to Bullseye update

Yescrypt is not supported by Debian 10 (buster). As a result, shadow password files (/etc/shadow) cannot be copied from a bullseye system back to a buster system. If these files are copied, passwords that have been changed on the bullseye system will not work on the buster system. Similarly, password hashes cannot be cut/pasted from a bullseye to a buster system.

If compatibility is required for password hashes between bullseye and buster, modify /etc/pam.d/common-password. Find the line that looks like:

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

and replace yescrypt with sha512.

5.1.4 NSS NIS and NIS+ support require new packages

NSS NIS and NIS+ support has been moved to separate packages called libnss-nis and libnss-nisplus. Unfortunately, glibc can’t depend on those packages, so they are now only recommended.

On systems using NIS or NIS+, it is therefore recommended to check that those packages are correctly installed after the upgrade.

5.1.5 Config file fragment handling in unbound

The DNS resolver unbound has changed the way it handles configuration file fragments. If you are relying on an include: directive to merge several fragments into a valid configuration, you should read the NEWS file (https://sources.debian.org/src/unbound/bullseye/debian/NEWS/).

5.1.6 rsync parameter deprecation

The rsync parameter --noatime has been renamed --open-noatime. The old form is no longer supported; if you are using it you should see the NEWS file (https://sources.debian.org/src/rsync/bullseye/debian/rsync.NEWS/). Transfer processes between systems running different Debian releases may require the buster side to be upgraded to a version of rsync from the backports (https://backports.debian.org/) repository. The version of rsync in the initial release of bullseye also deprecated --copy-devices in favor of --write-devices, but version 3.2.3-4+deb11u1 (included in bullseye point release 11.1) reverts this deprecation and supports both options.

5.1.7 Vim addons handling

The addons for vim historically provided by vim-scripts are now managed by Vim’s native „package” functionality rather than by vim-addon-manager. Vim users should prepare before upgrading by following the instructions in the NEWS file (https://sources.debian.org/src/vim-scripts/bullseye/debian/NEWS/).

5.1.8 OpenStack and cgroups v1

OpenStack Victoria (released in bullseye) requires cgroup v1 for block device QoS. Since bullseye also changes to using cgroupv2 by default (see Section 2.2.4), the sysfs tree in /sys/fs/cgroup will not include cgroup v1 features such as /sys/fs/cgroup/blkio, and as a result cgcreate -g blkio:foo will fail. For OpenStack nodes running nova-compute or cinder-volume, it is strongly advised to add the parameters systemd.unified_cgroup_hierarchy=false and systemd.legacy_systemd_cgroup_controllers to the kernel command line in order to override the default and restore the old cgroup hierarchy.

5.1.9 OpenStack API policy files

Following upstream’s recommendations, OpenStack Victoria as released in bullseye switches the OpenStack API to use the new YAML format. As a result, most OpenStack services, including Nova, Glance, and Keystone, appear broken with all of the API policies written explicitly in the policy.json files. Therefore, packages now come with a folder /etc/PROJECT/policy.d containing a file 00_default_policy.yaml, with all of the policies commented out by default.

To avoid the old policy.json file staying active, the Debian OpenStack packages now rename that file as disabled.policy.json.old. In some cases where nothing better could be done in time
for the release the policy.json is even simply deleted. So before upgrading, it is strongly advised to back up the policy.json files of your deployments.

More details are available in the upstream documentation (https://governance.openstack.org/tc/goals/selected/wallaby/migrate-policy-format-from-json-to-yaml.html).

5.1.10 sendmail downtime during upgrade

In contrast to normal upgrades of sendmail, during the upgrade of buster to bullseye the sendmail service will be stopped, causing more downtime than usual. For generic advice on reducing downtime see Section 4.1.3.

5.1.11 FUSE 3

Some packages including gvfs-fuse, kio-fuse, and sshfs have switched to FUSE 3. During upgrades, this will cause fuse3 to be installed and fuse to be removed.

In some exceptional circumstances, e.g., when performing the upgrade by only running apt-get dist-upgrade instead of the recommended upgrade steps from Cap. 4, packages depending on fuse3 might be kept back during upgrades. Running the steps discussed in Section 4.4.5 again with bullseye’s apt or upgrading them manually will resolve the situation.

5.1.12 GnuPG options file

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

5.1.13 Linux enables user namespaces by default

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

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

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

```
user.max_user_namespaces = 0
```

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

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

5.1.14 Linux disables unprivileged calls to bpf() by default

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

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

```
kernel.unprivileged_bpf_disabled = 0
```

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

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

5.1.16 **Exim 4.94**

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

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

Typical nonworking examples include:

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

- **Using**

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

  instead of

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

  for a virtual domain alias file.

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

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

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

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

5.1.17 **SCSI device probing is non-deterministic**

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

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

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

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

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

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

5.1.20 Upgrades involving libc1c2 need two runs

Packages that depend on libc1c2 in buster (e.g. guile-2.2-libs) may be held back during the first full upgrade run to bullseye. Doing a second upgrade normally solves the issue. The background of the issue can be found in bug #988963 (https://bugs.debian.org/988963).

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

The fail2ban package can be configured to send out e-mail notifications. It does that using mail, which is provided by multiple packages in Debian. A security update (needed on systems that use mail from mailutils) just before the release of bullseye broke this functionality for systems that have mail provided by bsd-mailx. Users of fail2ban in combination with bsd-mailx who wish fail2ban to send out e-mail should either switch to a different provider for mail or manually unapply the upstream commit (https://github.com/fail2ban/fail2ban/commit/410a6ce5c80dd981c22752da034f2529b5ee8d/) (which inserted the string ”-E 'set escape'“ in multiple places under /etc/fail2ban/action.

5.1.22 No new SSH connections possible during upgrade

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

5.1.23 Open vSwitch upgrade requires interfaces(5) change

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

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

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

5.1.24 Operațiuni de executat după actualizare și înainte de repornire.

Când `apt full-upgrade` s-a încheiat partea „formală” a actualizării este completă. Pentru actualizarea la bullseye nu sunt necesare operațiuni speciale înainte de repornire.

5.2 Items not limited to the upgrade process

5.2.1 Limitări în suportul de securitate

Există anumite pachete pentru care Debian nu poate promite furnizarea actualizărilor de securitate. Acestea sunt menționate în sub-secțiunile de mai jos.
5.2.1.1 Starea securității navigatoarelor web și a motoarelor de randare

Debian 11 includes several browser engines which are affected by a steady stream of security vulnerabilities. The high rate of vulnerabilities and partial lack of upstream support in the form of long term branches make it very difficult to support these browsers and engines with backported security fixes. Additionally, library interdependencies make it extremely difficult to update to newer upstream releases. Therefore, browsers built upon e.g. the webkit and khtml engines1 are included in bullseye, but not covered by security support. These browsers should not be used against untrusted websites. The webkit2gtk and wpewebkit engines are covered by security support.


5.2.1.2 OpenJDK 17

Debian bullseye comes with an early access version of OpenJDK 17 (the next expected OpenJDK LTS version after OpenJDK 11), to avoid the rather tedious bootstrap process. The plan is for OpenJDK 17 to receive an update in bullseye to the final upstream release announced for October 2021, followed by security updates on a best effort basis, but users should not expect to see updates for every quarterly upstream security update.

5.2.1.3 Go-based packages

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

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

5.2.2 Accesarea setărilor GNOME fără mouse

Fără un dispozitiv de indicare nu există o cale directă pentru a modifica setări în aplicația GNOME Settings din gnome-control-center. Pentru a ocoli problema puteți naviga din bara laterală la conținutul principal apăsând de două ori săgeată dreapta. Pentru a ajunge din nou în bara laterală puteți porni o căutare cu Ctrl + F, scrieți ceva, după care apăsați Esc pentru a anula căutarea. Acum puteți folosi săgeată sus și săgeată jos pentru a naviga în bara laterală. Rezultatele căutării nu se pot selecta cu tastatura.

5.2.3 The rescue boot option is unusable without a root password

With the implementation of sulogin used since buster, 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

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

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/bullseye/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/bullseye/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).

5.2.4 32-bit Xen PV guests are not supported

The Linux kernel (from version 5.9) no longer supports 32-bit xen virtual machines using PV mode (https://wiki.xenproject.org/wiki/Virtualization_Spectrum). Such virtual machines need to be converted to the 64-bit PC architecture.

You can check which mode a Xen guest is running (inside the virtual machine):

```
$ cat /sys/hypervisor/guest_type
PV
```

Virtual machines that return, for example, PVH or HVM are not affected.

5.3 Obsolescence and deprecation

5.3.1 Pachete notabile învechite

Mai jos urmează o listă de pachete învechite cunoscute și notabile (consultați Secțiune 4.8 pentru descriere).

Lista pachetelor învechite include:

- The `lilo` package has been removed from bullseye. The successor of lilo as boot loader is `grub2`.

- The Mailman mailing list manager suite version 3 is the only available version of Mailman in this release. Mailman has been split up into various components; the core is available in the package `mailman3` and the full suite can be obtained via the `mailman3-full` metapackage.

  The legacy Mailman version 2.1 is no longer available (this used to be the package `mailman`). This branch depends on Python 2 which is no longer available in Debian.

  For upgrading instructions, please see the project’s migration documentation. (https://docs.mailman3.org/en/latest/migration.html)

- The Linux kernel no longer provides `isdn4linux` (i4l) support. Consequently, the related userland packages `isdnutils`, `isdnactivecards`, `drdsl` and `ibod` have been removed from the archives.

- The deprecated `libappindicator` libraries are no longer provided. As a result, the related packages `libappindicator1`, `libappindicator3-1` and `libappindicator-dev` are no longer available. This is expected to cause dependency errors for third-party software that still depends on `libappindicator` to provide system tray and indicator support.

  Debian is using `libayatana-appindicator` as the successor of `libappindicator`. For technical background see this announcement (https://lists.debian.org/debian-devel/2018/03/msg00506.html).

- Debian no longer provides `chef`. If you use Chef for configuration management, the best upgrade path is probably to switch to using the packages provided by Chef Inc (https://www.chef.io/).

  For background on the removal, see the removal request (https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=963750).
5.4 Known severe bugs

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

- Python 2 is already beyond its End Of Life, and will receive no security updates. It is not supported for running applications, and packages relying on it have either been switched to Python 3 or removed. However, Debian bullseye does still include a version of Python 2.7, as well as a small number of Python 2 build tools such as python-setuptools. These are present only because they are required for a few application build processes that have not yet been converted to Python 3.

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

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

5.3.2 Componente depășite din bullseye

Odată cu următoarea lansare de Debian 12 (cu nume de cod bookworm) anumite funcții vor fi declareate învechite (n. trad. „deprecated”). Pentru a preveni probleme la actualizarea la Debian 12 utilizatorii ar trebui să migreze la soluții alternative.

Următoarele funcții sunt afectate:

- The historical justifications for the filesystem layout with /bin, /sbin, and /lib directories separate from their equivalents under /usr no longer apply today; see the Freedesktop.org summary (https://www.freedesktop.org/wiki/Software/systemd/TheCaseForTheUsrMerge). Debian bullseye will be the last Debian release that supports the non-merged/usr layout; for systems with a legacy layout that have been upgraded without a reinstall, the usrmmerge package exists to do the conversion if desired.

- bullseye is the final Debian release to ship apt-key. Keys should be managed by dropping files into /etc/apt/trusted.gpg.d instead, in binary format as created by gpg --export with a .gpg extension, or ASCII armored with a .asc extension.

A replacement for apt-key list to manually investigate the keyring is planned, but work has not started yet.

- The slapd database backends slapd-bdb (https://manpages.debian.org/bullseye/slapd/slapd-bdb.5.html), slapd-hdb (https://manpages.debian.org/bullseye/slapd/slapd-hdb.5.html), and slapd-shell (https://manpages.debian.org/bullseye/slapd/slapd-shell.5.html) are being retired and will not be included in Debian 12. LDAP databases using the bdb or hdb backends should be migrated to the slapd-mdb (https://manpages.debian.org/bullseye/slapd/slapd-mdb.5.html) backend.

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

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

5.4 Known severe bugs

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

<table>
<thead>
<tr>
<th>Bug number</th>
<th>Package (source or binary)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>922981</td>
<td>ca-certificates-java</td>
<td>ca-certificates-java: /etc/ca-certificates/update.d/jks-keystore doesn’t update /etc/ssl/certs/java/cacerts</td>
</tr>
<tr>
<td>990026</td>
<td>cron</td>
<td>cron: Reduced charset in MAILTO causes breakage</td>
</tr>
<tr>
<td>991081</td>
<td>gir1.2-didon-1.0</td>
<td>gir1.2-didon-1.0 lacks dependencies</td>
</tr>
<tr>
<td>990318</td>
<td>python-pkg-resources</td>
<td>python-pkg-resources: please add Breaks against the unversioned python packages</td>
</tr>
<tr>
<td>991449</td>
<td>fail2ban</td>
<td>fix for CVE-2021-32749 breaks systems with mail from bsd-mailx</td>
</tr>
<tr>
<td>990708</td>
<td>mariadb-server-10.5,galera</td>
<td>mariadb-server-10.5: upgrade problems due to galera-3 -&gt; galera-4 switch</td>
</tr>
<tr>
<td>980429</td>
<td>src:gcc-10</td>
<td>g++ + -10: spurious c++17 mode segmentation fault in append_to_statement_list_1 (tree-iterator.c:65)</td>
</tr>
<tr>
<td>980609</td>
<td>src:gcc-10</td>
<td>missing i386-cpuinfo.h</td>
</tr>
<tr>
<td>984574</td>
<td>gcc-10-base</td>
<td>gcc-10-base: please add Breaks: gcc-8-base (&lt; &lt; 8.4)</td>
</tr>
<tr>
<td>987264</td>
<td>git-el</td>
<td>git-el: fails to install with xemacs21</td>
</tr>
<tr>
<td>991082</td>
<td>gir1.2-gtd-1.0</td>
<td>gir1.2-gtd-1.0 has empty Depends</td>
</tr>
<tr>
<td>948739</td>
<td>gparted</td>
<td>gparted should not mask mount units</td>
</tr>
<tr>
<td>984714</td>
<td>gparted</td>
<td>gparted should suggest extatprows and backport the commit that rejects extat-utils</td>
</tr>
<tr>
<td>968368</td>
<td>ifenslave</td>
<td>ifenslave: Option bond-master fails to add interface to bond</td>
</tr>
<tr>
<td>990428</td>
<td>ifenslave</td>
<td>ifenslave: Bonding not working on bullseye (using bondslaves config)</td>
</tr>
<tr>
<td>991113</td>
<td>libpam-chroot</td>
<td>libpam-chroot installs pam_chroot.so into the wrong directory</td>
</tr>
<tr>
<td>989545</td>
<td>src:llvm-toolchain-11</td>
<td>libgl1-mesa-dri: si_texture.c:1727 si_texture_transfer_map - failed to create temporary texture to hold untilted copy</td>
</tr>
<tr>
<td>982459</td>
<td>mdadm</td>
<td>mdadm --examine in chroot without /proc/dev/sys mounted corrupts host's filesystem</td>
</tr>
<tr>
<td>Bug number</td>
<td>Package (source or binary)</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>981054</td>
<td>openipmi</td>
<td>openipmi: Missing dependency on kmod</td>
</tr>
<tr>
<td>948318</td>
<td>openssh-server</td>
<td>openssh-server: Unable to restart sshd restart after upgrade to version 8.1p1-2</td>
</tr>
<tr>
<td>991151</td>
<td>procs</td>
<td>procs: dropped the reload option from the init script, breaking corekeeper</td>
</tr>
<tr>
<td>989103</td>
<td>pulseaudio</td>
<td>pulseaudio regressed on control=Wave configuration</td>
</tr>
<tr>
<td>984580</td>
<td>libpython3.9-dev</td>
<td>libpython3.9-dev: missing dependency on zlib1g-dev</td>
</tr>
<tr>
<td>990417</td>
<td>src:qemu</td>
<td>openjdk-11-jre-headless: running java in qemu s390 gives a SIGILL at C [linux-vdso64.so.1+0x6f8] __kernel_getcpu+0x8</td>
</tr>
<tr>
<td>859926</td>
<td>speech-dispatcher</td>
<td>breaks with pulse-audio as output when spawned by speechd-up from init system</td>
</tr>
<tr>
<td>932501</td>
<td>src:squid-deb-proxy</td>
<td>squid-deb-proxy: daemon does not start due to the conf file not being allowed by apparmor</td>
</tr>
<tr>
<td>991588</td>
<td>tpm2-abrmd</td>
<td>tpm2-abrmd should not use Requires=systemd-udevd-settle.service in its unit</td>
</tr>
</tbody>
</table>
| 991939     | libjs-bootstrap4         | libjs-bootstrap4: broken symlinks: /usr/share/javascript/bootstrap/css/bootstrap*.css.map -> ../../../nodejs/bootstrap/dist/css/bootstrap*.css.map > ...
| 991822     | src:wine                 | src:wine: dh_auto_clean deletes unrelated files outside of package source |
| 988477     | src:xen                  | xen-hypervisor-4.14-amd64: xen dmesg shows (XEN) AMD- Vi: IO_PAGE_FAULT on sata pci device |
| 991788     | xfce4-settings           | xfce4-settings: black screen after suspend when laptop lid is closed and re-opened |
Capitolul 6

Mai multe informații despre Debian

6.1 Referințe suplimentare


Documentația pentru pachete individuale este instalată în `/usr/share/doc/pachet`. Aceasta poate include informații despre drepturile de autor, detalii specifice Debian, precum și documentația originală a pachetului.

6.2 Obținerea de ajutor

Există multe surse de ajutor, sfaturi și suport pentru utilizatorii Debian, însă acestea ar trebui considerate doar după cercetarea problemei în documentația disponibilă. Această secțiune oferă o scurtă introducere despre aceste surse, ce ar putea fi de ajutor noilor utilizatori Debian.

6.2.1 Listele de discuții


6.2.2 Internet Relay Chat


Pentru mai multe informații despre OFTC vă rugăm vizitați situl web (http://www.oftc.net/).

6.3 Raportarea problemelor

Dacă ați descoperit o problemă în distribuție sau în programele împachetate, vă rugăm să o raportați pentru ca aceasta să fie remediată în versiunile următoarele. Raportarea problemelor necesită o adresă de e-mail validă. Solicităm acest lucru pentru a putea urmări problemele și pentru ca dezvoltatorii să poată lua legătura cu cei care raportează problemele, în caz că au nevoie de mai multe informații.

Puteți trimite un raport de problemă folosind programul reportbug sau manual, folosind un e-mail. Puteți citi mai multe despre Sistemul de gestionare a problemelor și cum se poate utiliza citind documentația de referință (disponibilă în /usr/share/doc/debian dacă aveți instalat doc-debian) sau online la Bug Tracking System (https://bugs.debian.org/).

6.4 Contribuirea la Debian


În orice caz, dacă lucrați în orice fel în comunitatea software liber, ca utilizator, programator, autor de documentație sau traducător, ajutați deja efortul pentru software liber. Contribuțiile aduc satisfacții și bună dispoziție, și pe lângă oportunitatea de a cunoaște persoane noi creează un sentiment bun în interior.
Capitolul 7

Glosar

ACPI
Advanced Configuration and Power Interface (Interfață avansată pentru configurare și consum de curent)

ALSA
Advanced Linux Sound Architecture (Arhitectură Linux avansată pentru sunet)

BD
Blu-ray Disc

CD
Compact Disc

CD-ROM
Compact Disc Read Only Memory (Disc compact care poate fi doar citit)

DHCP
Dynamic Host Configuration Protocol (Protocol de configurare dinamică a calculatorului-gazdă)

DLBD
Dual Layer Blu-ray Disc (Disc Blu-ray de tip dublu-strat)

DNS
Domain Name System (Sistem de numire a domeniilor)

DVD
Digital Versatile Disc (Disc digital versatil)

GIMP
GNU Image Manipulation Program (Programul GNU pentru manipularea imaginilor)

GNU
GNU’s Not Unix (GNU Nu-i Unix)

GPG
GNU Privacy Guard (Gardă GNU pentru confidențialitate)

LDAP
Lightweight Directory Access Protocol (Protocol de categorie ușoară pentru accesarea registrului)

LSB
Linux Standard Base (Bază standardizată Linux)

LVM
Logical Volume Manager (Managerul de volume logice)

MTA
Mail Transport Agent (Agent de transport al mesajelor)
CAPITOLUL 7. GLOSAR

NBD
Network Block Device (Dispozitiv de tip bloc conectat prin rețea)

NFS
Network File System (Sistem de fișiere în rețea)

NIC
Network Interface Card (Placă de rețea)

NIS
Network Information Service (Serviciul de informații în rețea)

PHP
PHP: Hypertext Preprocessor (PHP: pre-procesor pentru hipertext)

RAID
Redundant Array of Independent Disks (Matrice redundanță de discuri independente)

SATA
Serial Advanced Technology Attachment (Ataşare serială cu tehnologie avansată)

SSL
Secure Sockets Layer (Strat de socluri securizat)

TLS
Transport Layer Security (Securitate a stratului de transport)

UEFI
Unified Extensible Firmware Interface (Interfață extensibilă unificată pentru microcod)

USB
Universal Serial Bus (Magistrală universală serială)

UUID
Universally Unique Identifier (Identificator unic universal)

WPA
Wi-Fi Protected Access (Acces Wi-Fi protejat)
Anexa A

Gestionarea sistemului buster înainte de actualizare

Această anexă conține informații despre cum să vă asigurați că puteți instala sau actualiza pachete buster înainte de a actualiza la bullseye. Acest lucru ar trebui să fie necesar doar în anumite situații.

A.1 Actualizarea sistemului buster

Practic aceasta nu este diferită de altă actualizare pe care ați efectuat-o pentru buster. Singura diferență este că trebuie să vă asigurați mai întâi că lista de pachete încă conține referințe către buster, după cum se explică în Section A.2.

Dacă actualizați sistemul folosind un sit-oglindă Debian, atunci sistemul va fi actualizat automat la ultima versiune intermediară de buster.

A.2 Verificarea fișierelor listelor de surse APT


Dacă deja ați instalat pachete din bullseye, probabil nu mai are rost să mai instalați pachete din buster. În acest caz va trebui să decideți dacă doriti să continuați sau nu. Este posibil să reveniți la versiuni anterioare ale pachetelor, însă acest subiect nu este acoperit aici.


Dacă aveți linii care încep cu deb file:sau URIs: file:, va trebui să verificați dacă locația la care se referă conține o arhivă buster sau bullseye.

**IMPORTANT**


Dacă ați efectuat modificări, salvați fișierul și executați

```
# apt update
```

pentru a actualiza lista de pachete.
A.3 Îndepărtarea fișierelor de configurare inutile

Înainte de a actualiza sistemul la bullseye este recomandat să ștergeți fișierele vechi de configurare (cum ar fi fișierele *.dpkg-*{new,old} din /etc) din sistem.
Anexa B

Contribuitorii la Notele de lansare

Multe persoane au contribuit la notele de lansare, printre care


Glosar

A
Apache, 4

B
BIND, 4

C
Calligra, 3
Cryptsetup, 4

D
DocBook XML, 2
Dovecot, 4

E
Exim, 4

G
GCC, 4
GIMP, 4
GNOME, 3
GNUcash, 4
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
apt, 2, 14, 25
apt-listchanges, 18
aptitude, 12, 17, 21
aufs-dkms, 30
bazel-bootstrap, 6
bsd-mailx, 27
cacertificates-java, 31
chef, 29
cinder-volume, 24
connman, 30
cron, 31
cups-browsed, 4
cups-daemon, 4
cups-filters, 4
dblatex, 2
debian-goodies, 17
debian-kernel-handbook, 21
debian-security-support, 28
doc-debian, 34
docbook-xsl, 2
dpkg, 1
drdsl, 29
exfat-fuse, 6
exfat-utils, 6
exfatprogs, 6
fail2ban, 27, 31
firmware-iwlwifi, 27
fuse, 25
fuse3, 25
gcc-10-base, 31
gir1.2-diodon-1.0, 31
gir1.2-gtd-1.0, 31
git, 31
lib, 24
gnome-control-center, 28
parted, 31
grub2, 29
guile-2.2-libs, 27
gvfs-fuse, 25
how-can-i-help, 34
ibod, 29
ifenslave, 31
initramfs-tools, 10, 20
intel-microcode, 27
ipp-usb, 4, 5
isdnactivecards, 29
isdnutils, 29
kio-fuse, 25
libappindicator-dev, 29
libappindicator1, 29
libappindicator3-1, 29
libyatana-appindicator, 29
libgc1c2, 27
libjs-bootstrap4, 32
libnss-nis, 24
libnss-nisplus, 24
libpam-chroot, 31
libpython3.9-dev, 32
libsane1, 5
lilo, 29
linux-image-*, 20
linux-image-amd64, 21
linux-source, 21
localepurge, 17
mailman, 29
mailman3, 29
mailman3-full, 29
mailutils, 27
mariadb-server-10.5,galera-4, 31
mdadm, 31
network-manager, 30
nova-compute, 24
openipmi, 32
openssh-server, 27, 32
openvswitch, 27
popularity-contest, 17
procps, 32
pulseaudio, 32
python-pkg-resources, 31
python-setuptools, 30
rails, 26
rdiff-backup, 26
redmine, 26
release-notes, 1
rsync, 24
rsyslog, 5
sane-airscan, 5
sendmail, 25
slapd, 30
speech-dispatcher, 32
src:gcc-10, 31
src:llvm-toolchain-11, 31
src:qemu, 32
src:qemu-ebf, 32
src:qemud, 32
src:qemu-ski, 32
src:xen, 32
sshfs, 25
synaptic, 12
systemd, 6
tinc, 11
tpm2-abrmd, 32
udev, 20, 26
unbound, 24
upgrade-reports, 1
usrmerge, 30
vim, 24
vim-addon-manager, 24
vim-scripts, 24
wiced, 30
xen, 29
xfce4-settings, 32
xmlroff, 2
xsltproc, 2
Perl, 4
PHP, 4
Postfix, 4
PostgreSQL, 4
X
Xfce, 3