Uwagi do wydania, do dystrybucji Debian 11 (bullseye), System z

The Debian Documentation Project (https://www.debian.org/doc/)

19 lipca 2022
Uwagi do wydania, do dystrybucji Debian 11 (bullseye), System z

Niniejszy dokument jest wolnym oprogramowaniem. Można go rozpowszechniać i/lub modyfikować zgodnie z warunkami Licencji Publicznej GNU w wersji 2, opublikowanej przez Fundację Wolnego Oprogramowania.

Niniejszy program rozpowszechniany jest w nadziei, iż będzie on użyteczny - jednak BEZ JAKIEJKOLWIEK GWARANCJI, nawet domyślnej gwarancji PRZYDATNOŚCI HANDLOWEJ albo PRZYDATNOŚCI DO OKREŚLONYCH ZASTOSOWAŃ. Więcej informacji zawiera Powszechna Licencja Publiczna GNU.

Do niniejszego dokumentu powinien być dołączony egzemplarz Powszechnej Licencji Publicznej GNU (GNU General Public License); jeśli nie - proszę napisać do Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

The license text can also be found at https://www.gnu.org/licenses/gpl-2.0.html and /usr/share/common-licenses/GPL-2 on Debian systems.
4.4.2 Aktualizowanie listy pakietów ................................................. 16
4.4.3 Zapewnienie wystarczającej ilości wolnego miejsca ...................... 16
4.4.4 Minimalna aktualizacja systemu ............................................. 18
4.4.5 Aktualizacja systemu ........................................................... 19
4.5 Możliwe problemy przy aktualizacji ............................................ 19
  4.5.1 Podczas aktualizacji dystrybucji pojawia się błąd „Nie udało się wykonać natych-
  miastowej konfiguracji” ....................................................... 19
4.5.2 Spodziewane usunięcia pakietów ............................................ 19
4.5.3 Konflikty lub pętle „wymaga wstępnie” .................................... 19
4.5.4 Konflikty plików .................................................................. 20
4.5.5 Zmiany konfiguracji ............................................................. 20
4.5.6 Zmiany sesji na konsoli ......................................................... 20
4.6 Aktualizacja jądra i powiązanych pakietów ................................... 20
  4.6.1 Instalowanie metapakietu jądra ............................................. 20
4.7 Przygotowanie do kolejnego wydania ........................................... 21
  4.7.1 Czyszczenie usuniętych pakietów ......................................... 21
4.8 Przestarzałe pakiety .................................................................... 22
  4.8.1 Transitional dummy packages ............................................. 22

5 Problemy, które należy mieć na uwadze, a dotyczące wydania bullseye 25
  5.1 Uwagi dotyczące aktualizacji do bullseye ................................... 25
  5.1.1 The XFS file system no longer supports barrier/nobarrier option .... 25
  5.1.2 Changed security archive layout ......................................... 25
  5.1.3 Password hashing uses yescrypt by default .......................... 25
  5.1.4 NSS NIS and NIS+ support require new packages .................. 26
  5.1.5 Config file fragment handling in unbound ............................. 26
  5.1.6 rsync parameter deprecation ............................................. 26
  5.1.7 Vim addons handling ......................................................... 26
  5.1.8 OpenStack and cgroups v1 ................................................. 26
  5.1.9 OpenStack API policy files ............................................... 26
  5.1.10 sendmail downtime during upgrade .................................... 27
  5.1.11 FUSE 3 ........................................................................ 27
  5.1.12 GnuPG options file ......................................................... 27
  5.1.13 Linux enables user namespaces by default ......................... 27
  5.1.14 Linux disables unprivileged calls to bpf() by default ............ 27
  5.1.15 redmine missing in bullseye ............................................. 28
  5.1.16 Exim 4.94 ..................................................................... 28
  5.1.17 SCSI device probing is non-deterministic ......................... 28
  5.1.18 rdiff-backup require lockstep upgrade of server and client .... 28
  5.1.19 Intel CPU microcode issues ............................................. 29
  5.1.20 Upgrades involving libgc1c2 need two runs ....................... 29
  5.1.21 fail2ban can't send e-mail using mail from bsd-mailx .......... 29
  5.1.22 No new SSH connections possible during upgrade .......... 29
  5.1.23 Open vSwitch upgrade requires interfaces(5) change ....... 29
  5.1.24 Sprawy do zrobienia przed ponownym uruchomieniem ....... 29

  5.2 Items not limited to the upgrade process .................................. 30
  5.2.1 Ograniczenia we wsparciu bezpieczeństwa .......................... 30
  5.2.1.1 Security status of web browsers and their rendering engines .. 30
  5.2.1.2 OpenJDK 17 ................................................................ 30
  5.2.1.3 Go-based packages ..................................................... 30
  5.2.2 Accessing GNOME Settings app without mouse .................... 30
  5.2.3 The rescue boot option is unusable without a root password .... 31

  5.3 Obsolescence and deprecation ................................................. 31
  5.3.1 Znane pakieti oznaczone jako przestarzałe .......................... 31
  5.3.2 Przestarzałe składniki w wydaniu bullseye ......................... 32

  5.4 Known severe bugs ............................................................... 32
6 Więcej informacji na temat projektu Debian
   6.1 Dodatkowe informacje ................................................................. 35
   6.2 Pomoc ......................................................................................... 35
      6.2.1 Listy dyskusyjne ................................................................. 35
      6.2.2 IRC ......................................................................................... 35
   6.3 Zgłaszanie błędów ................................................................. 36
   6.4 Uczestnictwo w rozwoju Debiana ......................................... 36

7 Glossary ..................................................................................... 37

A Zarządzanie wydaniem buster przed aktualizacją .......................... 39
   A.1 Uaktualnienie wydania buster ................................................. 39
   A.2 Checking your APT source-list files ........................................ 39
   A.3 Usunięcie przestarzałych plików konfiguracyjnych .................. 40

B Współtwórcy uwag do wydania ................................................. 41

Indeks ......................................................................................... 43
Rozdział 1

Wstęp

Niniejszy dokument informuje użytkowników dystrybucji Debian o głównych zmianach w wersji 11 (nazwa kodowa bullseye).

Informacje o wydaniu zawierają wskazówki na temat bezpiecznej aktualizacji z wydania 10 (nazwa kodowa buster) do wydania bieżącego oraz informacje o znanych, ewentualnych błędach, na które mogą natknąć się użytkownicy w trakcie tego procesu.

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

**UWAGA!**

Proszę zwrócić uwagę, że nie jest to opis wszystkich znanych błędów, a tylko wybór, który opiera się na przewidywanej ilości ich wystąpienia oraz ewentualnych następstwach.

Proszę zauważyć, że wspierana i dokumentowana jest jedynie aktualizacja z poprzedniej wersji Debianna (buster). W przypadku aktualizacji ze starszych wydań, sugerujemy uprzednie zapoznanie się z poprzednią wersją informacji o wydaniu i aktualizację do Debianna buster.

1.1 Zgłaszanie błędów w tym dokumencie

Staraliśmy się przetestować wszystkie możliwe kombinacje poszczególnych kroków aktualizacji opisanych w tym dokumencie oraz przewidzieć błędy, na jakie mogą natrafić użytkownicy tej wersji dystrybucji.

W przypadku znalezienia błędów (nieprawidłowej bądź brakującej informacji w dokumencie), proszę zgłosić to w [systemie śledzenia błędów](https://bugs.debian.org/) wobec pakietu `release-notes` (w języku angielskim). Wczesniej można przejrzeć [listę zauważonych błędów](https://bugs.debian.org/release-notes), aby uniknąć duplikowania zgłoszeń. Proszę dodawać informację do istniejących wpisów, jeśli poprawi to i uzupełni zawartość zgłoszeń. Informacje o błędach w samym tłumaczeniu uwag do wydania prosimy przesyłać na polskojęzyczną listę debian-l10n-polish.

Cenimy i zalecamy zgłaszanie łatek do źródeł tego dokumentu. Więcej informacji o pobieraniu ich można znaleźć w Sekcji 1.3.

1.2 Wysyłanie sprawozdań aktualizacji

Z chęcią przyjmiemy każdą informację (w języku angielskim) dotyczącą aktualizacji z wydania buster do bullseye. Aby przesyłać te informacje, proszę zgłosić błąd w [systemie śledzenia błędów](https://bugs.debian.org/) w odniesieniu do pakietu `upgrade-reports` dołączając swoje wyniki. Prosimy skompresować załączniki, używając do tego programu `gzip`.

Do zgłoszenia prosimy załączyć następujące informacje:
ROZDZIAŁ 1. WSTĘP

1.3 źródła niniejszego dokumentu

- Status bazy pakietów przed i po aktualizacji: status bazy danych dpkg dostępny w /var/lib/dpkg/status i informacje o stanie pakietów apt, zawarte w pliku /var/lib/apt/extended_states. Przed aktualizacją powinno się wykonać kopię zapasową, zgodnie z Sekcja 4.1.1, lecz kopię /var/lib/dpkg/status można znaleźć również w /var/backups.

- Logi sesji utworzone za pomocą script, zgodnie z opisem w Sekcja 4.4.1.

- Logi menedżera apt dostępne w /var/log/apt/term.log lub dzienniki aptitude, z /var/log/aptitude.

NOTATKA

Przed umieszczeniem logów, powinno się poświęcić nieco czasu na usunięcie z nich wszystkich prywatnych i/lub poufnych informacji, ponieważ zostaną one udostępnione w publicznej bazie danych.

1.3 Źródła niniejszego dokumentu

The source of this document is in DocBook XML format. The HTML version is generated using docbook-xsl and xsltproc. The PDF version is generated using dblatex or xmlroff. Sources for the Release Notes are available in the Git repository of the Debian Documentation Project. You can use the web interface (https://salsa.debian.org/ddp-team/release-notes/) to access its files individually through the web and see their changes. For more information on how to access Git please consult the Debian Documentation Project VCS information pages (https://www.debian.org/doc/vcs).
Rozdział 2

Nowości w dystrybucji Debian 11

The Wiki (https://wiki.debian.org/NewInBullseye) has more information about this topic.

2.1 Obsługiwane architektury

Architektury oficjalnie wspierane przez dystrybucję Debian 11:

- Komputery 32-bitowe (i386) i 64-bitowe (amd64) typu PC
- 64-bitowe ARM (arm64)
- ARM EABI (armel)
- ARMv7 (EABI hard-float ABI, armhf)
- little-endian MIPS (mipsel)
- 64-bitowe MIPS little-endian (mips64el)
- 64-bitowe PowerPC little-endian (ppc64el)
- IBM System z (s390x)

Więcej o statusie portów i informacjach charakteryzujących porty można przeczytać na Stronach o portach Debiana (https://www.debian.org/ports/).

2.2 Co nowego w dystrybucji?

Nowe wydanie Debiana zawiera więcej programów niż poprzednie. Obecna dystrybucja zawiera ponad 11294 nowych pakietów, z ogólnej liczby 59551 w tym wydaniu. Większość oprogramowania została zaktualizowana (ponad 42821 pakietów, co stanowi 72% wszystkich pakietów w buster). Znaczna liczba pakietów (ponad 9519, 16% pakietów w buster) została z różnych powodów usunięta z dystrybucji. W przypadku tych pakietów nie będą widoczne żadne aktualizacje. Zostaną one również oznaczone jako „przestarzałe” w interfejsach zarządzania pakietami (więcej w Sekcja 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.

Zaktualizowano również pakiety biurowe:

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

Pozna wieloma innymi, to wydanie zawiera następujące aktualizacje oprogramowania:
ROZDZIAŁ 2. NOWOŚCI W DYSTRYBUCJI ...

2.2. CO NOWEGO W DYSTRYBUCJI?

<table>
<thead>
<tr>
<th>Pakiet</th>
<th>Wersja w 10 (buster)</th>
<th>Wersja w 11 (bullseye)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache</td>
<td>2.4.38</td>
<td>2.4.48</td>
</tr>
<tr>
<td>Serwer 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>Domyślny serwer pocztowy Exim</td>
<td>4.92</td>
<td>4.94</td>
</tr>
<tr>
<td>GNU Compiler Collection jako domyślny kompilator</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>Biblioteka C GNU</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>Obraz jądra Linux</td>
<td>4.19 series</td>
<td>5.10 series</td>
</tr>
<tr>
<td>LLVM/Clang toolchain</td>
<td>6.0.1 and 7.0.1 (default)</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-what's-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.
ROZDZIAŁ 2. NOWOŚCI W DYSTRYBUCJI ...

2.2. CO NOWEGO W DYSTRYBUCJI?

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 libsanet 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) 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 Sekcja 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-journal.service(8) 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.

2.2.7 Wieści z odmiany 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. 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 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 init systems. 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).
Rozdział 3

System instalacyjny

Instalator Debiana (Debian Installer) jest oficjalnym systemem instalacji w przypadku Debiana. Oferuje on wiele metod instalacji. To, które z nich dostępne, zależy od używanej architektury.

Obrazy instalatora wydania bullseye są dostępne razem z przewodnikiem po instalacji na stronach Debiana (https://www.debian.org/releases/bullseye/debian-installer/).

The Installation Guide is also included on the first media of the official Debian DVD (CD/blu-ray) sets, at:

/doc/install/manual/język/index.html

Można również zapoznać się z errata (https://www.debian.org/releases/bullseye/debian-installer/index#errata) programu debian-installer, aby poznać listę znanych błędów.

3.1 Co nowego w systemie instalacyjnym?

There has been a lot of development on the Debian Installer since its previous official release with Debian 10, resulting in improved hardware support and some exciting new features or improvements.

If you are interested in an overview of the detailed changes since buster, please check the release announcements for the bullseye beta and RC releases available from the Debian Installer’s news history (https://www.debian.org/devel/debian-installer/News/).

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 Instalacja automatyczna

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.

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).
Rozdział 4

Aktualizacja z Debiana 10 (buster)

4.1 Przygotowanie do aktualizacji

Przed aktualizacją zalecamy zapoznanie się z informacjami zawartymi w Rozdział 5. Rozdział ten opisuje również potencjalne trudności, niezwiązane bezpośrednio z procesem aktualizacji, o których warto wiedzieć przed rozpoczęciem całej procedury.

4.1.1 Kopia zapasowa danych i konfiguracji

Przed zaktualizowaniem systemu zalecamy wykonanie pełnej kopii zapasowej, a przynajmniej kopii tych danych i konfiguracji, których utrata byłaby dla nas bolesna. Narzędzia i proces aktualizacji są dość niezawodne, lecz problem sprzętu w trakcie procedury może spowodować znaczne uszkodzenie systemu.


Sam proces aktualizacji nie zmienia niczego w katalogu /home. Niektóre aplikacje (np. część zestawu Mozilla oraz środowiska graficzne GNOME i KDE) nadpisują istniejące ustawienia użytkownika wartościami domyelnymi, gdy użytkownik uruchamia dany program jako pierwszy. Środkiem ostróżności jest wykonanie kopii zapasowych ukrytych plików i katalogów (z kropką - „dotfiles”) z katalogów domowych użytkowników. Ta kopia może ułatwić odzyskanie lub przywrócenie starych ustawień. Powinno się również poinformować o tym pozostałych użytkowników.

Operacja związana z instalacją pakietów musi być wykonana z uprawnieniami administratora, dlatego należy się zalogować na konto root, używając polecenia su lub wykorzystując sudo do uzyskania potrzebnych uprawnień.

Przed aktualizacją należy wykonać kilka czynności, dlatego trzeba zapoznać się z poniższą listą:

4.1.2 Uprzednie ostrzeżenie użytkowników

Przed każdą aktualizacją powinno się poinformować innych użytkowników systemu o tym fakcie, choć osoby uzyskujące dostęp do komputera za pomocą ssh nie powinny napotkać większych problemów podczas kontynuowania pracy.

Jako dodatkowe zabezpieczenie można wykonać przed wykonaniem aktualizacji kopię zapasową lub odmontować partycję z katalogiem /home.

Przy aktualizacji do wydania bullseye konieczne jest zaktualizowanie jądra. Nie obędzie się więc bez ponownego uruchomienia komputera. Zwykle odbywa się to po zakończeniu aktualizacji.

4.1.3 Przygotowanie do przestroju usług

Mogą istnieć usługi oferowane przez system, które są związane z pakietami objętymi aktualizacją. W takim przypadku proszę pamiętać, że podczas aktualizacji i konfiguracji będą one zatrzymane na czas zastąpienia ich przez nowszą wersję oraz nie będą w tym czasie dostępne.
ROZDZIAŁ 4. AKTUALIZACJA Z DEBIANA 10 …
4.1. PRZYGOTOWANIE DO AKTUALIZACJI

Dokładny czas braku dostępu do usług zależy od liczby aktualizowanych pakietów i od okresu, w jakim administrator odpowie na pytania konfiguracyjne. Proszę zwrócić uwagę, że jeśli proces aktualizacji nie będzie nadzorowany, a system będzie wymagał reakcji administratora, występuje duże prawdopodobieństwo trwania usług niedostępnych1 w dłuższym okresie.

Jeśli aktualizowany system udostępnia usługi, które są krytyczne dla użytkowników bądź sieci2, można ograniczyć przerwę w ich działaniu wykonując aktualizację minimalną (zgodnie z opisem w Sekcji 4.4.4) a następnie wykonać aktualizację jądra i ponownie uruchomić komputer (aktualizując pakiety związane z krytycznymi usługami). Dopiero później należy wykonać pełną aktualizację opisaną w Sekcji 4.4.5. W ten sposób można sprawdzić, że krytyczne usługi działają i są dostępne w trakcie pełnej aktualizacji, a przerwa w działaniu będzie zminimalizowana.

4.1.4 Przygotowanie do odzyskiwania

Choć Debian stara się zapewnić, że system będzie się uruchamiał w każdym przypadku to zawsze istnieje możliwość, że wystąpią problemy z ponownym jego uruchomieniem po dokonaniu aktualizacji. Rozpoznane, ewentualne problemy są omówione w tym i kolejnych rozdziałach uwag do wydania.

Z tego względu należy się upewnić, że będzie istniała możliwość odzyskania systemu jeśli nie uruchomiono go po aktualizacji (lub w przypadku systemów zarządzanych zdalnie nie zaktyniajie sieci).

W przypadku aktualizacji zdalnej za pomocą ssh, zaleca się dodatkowe środki bezpieczeństwa, w celu zapewnienia sobie możliwości dostępu do serwera za pomocą zdalnego terminala szeregowego. Istnieje ryzyko, że po aktualizacji jądra i ponownym uruchomieniu systemu wystąpi konieczność poprawienia konfiguracji systemu korzystając z konsoli lokalnej. Jeśli w trakcie aktualizacji system zostanie przypadkowo zresetowany, możliwe że konieczne będzie odzyskiwanie za pomocą lokalnej konsoli.


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 Debugowanie powłoki podczas rozruchu przy użyciu initrd

Pakiet initramfs-tools udostępnia powłokę debugowania3 w generowanych obrazach initrd. Na przykład: jeśli initrd nie będzie mógł zamontować głównego systemu plików to przeniesie się do powłoki debugowania z dostępowymi polecami, aby dać możliwość znalezienia problemu i naprawy.

Podstawowymi sprawami do sprawdzenia są: obecność poprawnych plików urządzeń w /dev; które moduły są załadowane (cat /proc/modules); wynik dmesg pod kątem błędów ładowania sterowników. Wykon dmesg pokaże również jakie pliki urządzeń zostały przypisane do danych dysków; powinno je się sprawdzić z wynikiem echo $ROOT, aby upewnić się, że główny system plików znajduje się na oczekiwanym urządzeniu.

Jeśli problem się rozwiąże to polecenie exit zamknie powłokę debugowania i proces debugowania będzie kontynuowany od momentu wystąpienia błędu. Oczywiście, konieczne będzie naprawienie źródła problemu i ponowne wygenerowanie initrd, aby przy następnym rozruchu nie znaleźć się w identycznej sytuacji.

4.1.4.2 Debugowanie powłoki podczas rozruchu przy użyciu systemd

Jeśli rozruch nie powiedzie się korzystający z systemd, można dostać się do powłoki roota służącej do debugowania zmieniając wiersz polecenia jądra. Jeśli podstawowy rozruch uda się, lecz część usług nie wystartuje, można spróbować dodać do parametrów jądra systemd.unit=--rescue.target.

1Jeśli priorytet debconf jest ustawiony na bardzo wysoką wartość, to może to spowodować niewyświetlanie pytania konfiguracyjnych. Usługi zależne od domyślnych odpowiedzi, które nie będą pasowały do danego systemu, nie uruchomiony się.
2Przykład: usługi DNS i DHCP, szczególnie jeśli nie ma redundancji lub tzw. failover. W przypadku DHCP użytkownicy mogą zostać odfacjowani z sieci, jeśli czas dzierżawy jest mniejszy niż czas trwania aktualizacji.
3Można wyłączyć tę funkcję dodając parametr panic=0 do parametrów rozruchowych.
Z kolei parametr jądra `systemd.unit=emergency.target` udostępnii powłokę roota najwcześniejszy jak to możliwe. Będzie to jednak jeszcze przed zamontowaniem głównego systemu plików z uprawnieniami do odczytu i zapisu. Zajdzie konieczność ręcznego wykonania:

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

More information on debugging a broken boot under systemd can be found in the Diagnosing Boot Problems (https://freedesktop.org/wiki/Software/systemd/Debugging/) article.

### 4.1.5 Przygotowanie bezpiecznego środowiska do uaktualnienia

**WAŻNE**

If you are using some VPN services (such as `tinc`) consider that they might not be available throughout the upgrade process. Please see Sekcja 4.1.3.

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

### 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.

The main configuration file that APT uses to decide what sources it should download packages from is `/etc/apt/sources.list`, but it can also use files in the `/etc/apt/sources.list.d/` directory - for details see sources.list(5) (https://manpages.debian.org//bullseye/apt/sources.list.5.html). If your system is using multiple source-list files then you will need to ensure they stay consistent.

#### 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

Below there are two methods for finding installed packages that did not come from Debian, using either `aptitude` or `apt-forktracer`. Please note that neither of them are 100% accurate (e.g. the aptitude example will list packages that were once provided by Debian but no longer are, such as old kernel packages).

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

```
# 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 Sekcja 5.1.2.

4.2.8 Sekcja proposed-updates

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

4.2.9 Nieoficjalne źródła

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

Część użytkowników może posiadać nieoficjalne, backportowane wersje pakietów, które są „nowsze” niż pakiety zainstalowane w Debianie buster. Te pakiety będą prawdopodobnie sprawiać kłopoty z powodu konfliktów plików⁴. Sekcja 4.5 opisuje sposoby rozwiązywania konfliktów plików.

4.2.10 Wyłączenie priorytetów APT-a (APT pinning)

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).

⁴System zarządzania pakietami Debiana nie pozwala zwykle na usunięcie lub zastąpienie pliku będącego własnością innego pakietu, chyba że pakiet został zdefiniowany jako zastępujący dany pakiet.
### 4.2.11 Check package status

Niezależnie od wybranej metody aktualizacji zaleca się uprzednie sprawdzenie wszystkich pakietów i zweryfikowanie czy wszystkie nadają się do aktualizacji. Następujące polecenie pokaże pakiety o statusie „częściowo zainstalowany” lub „nieprawidłowa konfiguracja” i te z jakimkolwiek statusem błędu:

```
# dpkg --audit
```

Można również sprawdzić stan wszystkich pakietów za pomocą `aptitude` lub np.:

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

Albo:

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

Pożądane może okazać się usunięcie wszelkich zatrzymań z pakietów. Jeśli jakikolwiek aktualizowany pakiet o statusie „istotny” będzie zatrzymany to aktualizacja nie powiedzie się.

Note that `aptitude` uses a different method for registering packages that are on hold than `apt` and `dselect`. You can identify packages on hold for `aptitude` with

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

If you want to check which packages you had on hold for `apt`, you should use

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

Jeśli zmieniono jakiś pakiet lub ponownie skompilowano go lokalnie bez zmiany nazwy ani dodania epoki do nazwy, konieczne będzie zatrzymanie go, aby zapobiec uaktualnieniu.

The „hold” package state for `apt` can be changed using:

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

Proszę zastąpić `hold` słowem `install` aby cofnąć „zatrzymanie” pakietu.

If there is anything you need to fix, it is best to make sure your APT source-list files still refer to buster as explained in Sekcja A.2.

### 4.3 Preparing APT source-list files

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 will consider all packages that can be found via any configured archive, and install the package with the highest version number, giving priority to the first entry in the files. Thus, if you have multiple mirror locations, list first the ones on local hard disks, then CD-ROMs, and then remote mirrors.

Wydanie można określić dzięki nazwie kodowej (np. `buster`, `bullseye`) lub statusowi wydania (oldstable · stare stabilne, stable · stabilne, testing · testowe, unstable · niestabilne). Zapis odnoszący się do nazwy kodowej ma tę zaletę, że użytkownik nie zostanie nigdy zaskoczony nowym wydaniem. Z tego powodu to rozwiązanie jest preferowane w niniejszym dokumencie. Z drugiej strony, powoduje to konieczność samodzielnego sprawdzania czy nie wydano nowej wersji systemu. Jeśli użyje się nazwy statusu pokaże się wówczas bardzo dużo dostępnych aktualizacji pakietów.

Debian udostępnia dwie listy dyskusyjne z ogłoszeniami, aby ułatwić bieżące śledzenie ważnych informacji związanych z wydaniami Debiana:

- By subscribing to the Debian announcement mailing list (https://lists.debian.org/debian-announce) you will receive a notification every time Debian makes a new release. Such as when `bullseye` changes from e.g. `testing` to `stable`. 

13
4.3. PREPARING APT SOURCE-LIST FILES

- Po zapisaniu się do listy dyskusyjnej z ogłoszeniami związanymi z bezpieczeństwem Debi ana (https://lists.debian.org/debian-announce/), będzie można śledzić wszystkie ogłoszenia bezpieczeństwa publikowane przez Debiana.

4.3.1 Dodanie internetowych źródeł APT-a

On new installations the default is for APT to be set up to use the Debian APT CDN service, which should ensure that packages are automatically downloaded from a server near you in network terms. As this is a relatively new service, older installations may have configuration that still points to one of the main Debian Internet servers or one of the mirrors. If you haven’t done so yet, it is recommended to switch over to the use of the CDN service in your APT configuration.

To make use of the CDN service, add a line like this to your APT source configuration (assuming you are using main and contrib):

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

After adding your new sources, disable the previously existing „deb” lines by placing a hash sign (#) in front of them.

However, if you get better results using a specific mirror that is close to you in network terms, this option is still available.

Debian mirror addresses can be found at https://www.debian.org/distrib/ftplist (look at the „list of Debian mirrors” section).

Załóżmy na przykład, że najbliższym serwerem lustrzanym jest http://mirrors.kernel.org. Przy sprawdzaniu go przeglądarką internetową można zauważyć, że główne katalogi są ułożone podobnie do:

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

To configure APT to use a given mirror, add a line like this (again, assuming you are using main and contrib):

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

Proszę zwrócić uwagę, że „dists” jest dodane jawnie, a argumenty po nazwie wydania są używane do rozwinięcia ścieżki na wiele katalogów.

Again, after adding your new sources, disable the previously existing archive entries.

4.3.2 Dodanie źródeł APT-a do lokalnego serwera lustrzanego

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

Kopia serwera lustrzanego może się znajdować np. w /var/local/debian/ i posiadać główne katalogi, takie jak:

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

Aby użyć jej ze swoim aptem, proszę dodać ten wiersz do pliku sources.list:

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

Proszę zwrócić uwagę, że „dists” jest dodane jawnie, a argumenty po nazwie wydania są używane do rozwinięcia ścieżki na wiele katalogów.

After adding your new sources, disable the previously existing archive entries in the APT source-list files by placing a hash sign (#) in front of them.
4.3.3 Dodanie źródeł APT-a do nośników optycznych

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

Proszę upewnić się, że w pliku /etc/fstab istnieje wiersz pozwalający na zamontowanie CD-ROM-u w punkcie montowania /media/cdrom. Na przykład, jeśli napęd CD-ROM jest urządzeniem /dev/sr0, to plik /etc/fstab powinien zawierać wiersz podobny do poniższego:

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

Proszę zauważyć, że w czwartym polu, między słowami noauto,ro nie mogą występować spacje. Aby sprawdzić, czy wszystko działa, proszę włożyć płytę i spróbować wykonac:

# mount /media/cdrom
# ls -aFl /media/cdrom
# umount /media/cdrom

Następnie, proszę uruchomić:

# apt-cdrom add
dla każdej płyty binarnej Debiana, aby dodać dane z każdego CD do bazy danych APT-a.

4.4 Aktualizacja pakietów

The recommended way to upgrade from previous Debian releases is to use the package management tool apt.

**NOTATKA**

**apt** is meant for interactive use, and should not be used in scripts. In scripts one should use **apt-get**, which has a stable output better suitable for parsing.

Proszę nie zapomnieć o zamontowaniu potrzebnych partycji do odczytu i zapisu (przede wszystkim partycji głównej /usr), za pomocą polecenia podobnego do poniższego:

# mount -o remount,rw /mountpoint

Next you should double-check that the APT source entries (in /etc/apt/sources.list and files under /etc/apt/sources.list.d/) refer either to "bullseye" or to "stable". There should not be any sources entries pointing to buster.

**NOTATKA**

Wiersze źródeł CD-ROM-u mogą niekiedy wskazywać na "unstable"; choć może być to mylące, nie należy tego zmieniać.

4.4.1 Zapisanie sesji

Zaleca się skorzystanie z programu /usr/bin/script, aby zapisać wyniki sesji aktualizacji. Wówczas, jeśli wystąpi problem, gotowy będzie log, który będzie można wykorzystać np. do zgłoszenia błędu. Aby rozpocząć zapisywanie, proszę wpisać:
lub coś podobnego. Jeśli będzie trzeba uruchomić zapis ponownie (np. po ponownym uruchomieniu systemu), proszę użyć innej wartości `krok`, aby wskazać zapisywanany krok aktualizacji. Nie należy umieszczać pliku (do którego będzie się zapisywało) w katalogu tymczasowym, takim jak `/tmp` lub `/var/tmp`. Pliki w tych katalogach będą usuwane przy aktualizacjach i po restartie.

Zapis ten pozwoli również na przeczytanie informacji, które już zniknęły z ekranu. Jeśli jest się w konsoli systemowej wystarczy przełączyć się do VT2 (za pomocą Alt+F2) i (po zalogowaniu się) skorzystać z polecenia `less -R ~root/upgrade-bullseye.script`, aby przejść plik.

Po zakończeniu aktualizacji można zatrzymać polecenie `script` poleceniem `exit`.

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

Jeśli użyto przełącznika `-t` do polecenia `script` można skorzystać z programu `scriptreplay`, aby od tworzyć całą sesję:

```
# scriptreplay ~/upgrade-bullseye.step.time ~/upgrade-bullseye.step.script
```

### 4.4.2 Aktualizowanie listy pakietów

Na początku, należy pobrać listę dostępnych pakietów nowego wydania. Można to zrobić za pomocą polecenia:

```
# apt update
```

**Notatka**

*Users of apt-secure may find issues when using aptitude or apt-get. For apt-get, you can use apt-get update --allow-releaseinfo-change.*

### 4.4.3 Zapewnienie wystarczającej ilości wolnego miejsca

Konieczne jest upewnienie się, że system posiada wystarczająco dużo wolnej przestrzeni dyskowej przed pełną aktualizacją systemu, opisaną w Sekcja 4.4.5. Wszystkie pakiety potrzebne do instalacji są najpierw pobierane z sieci i przechowywane w `/var/cache/apt/archives` (przy pobieraniu w podkatalogu `partial/`), dlatego trzeba zapewnić sobie wolne miejsce na partycji z katalogiem `/var/`. Po zakończeniu pobierania wolne miejsce potrzebne będzie na innych partycjach, aby zainstalować aktualizowane pakiety (które mogą zawierać większe pliki wykonywalne lub więcej danych) i nowe pakiety, pobrane przy aktualizacji. Jeśli jest zbyt mało wolnego miejsca można doprowadzić do trudnej w opanowaniu, niedokończonej aktualizacji.

`apt` can show you detailed information about the disk space needed for the installation. Before executing the upgrade, you can see this estimate by running:

```
# apt -o APT::Get::Trivial-Only=true full-upgrade
[...]
XXX upgraded, XXX newly installed, XXX to remove and XXX not upgraded.
Need to get xx.xMB of archives.
After this operation, AAAMB of additional disk space will be used.
```
If you do not have enough space for the upgrade, apt will warn you with a message like this:

E: You don’t have enough free space in /var/cache/apt/archives/.

W takim przypadku, konieczne będzie zwolnienie miejsca na dysku. Można:

- Remove packages that have been previously downloaded for installation (at /var/cache/apt/archives). Cleaning up the package cache by running apt clean will remove all previously downloaded package files.

- Remove forgotten packages. If you have used aptitude or apt to manually install packages in buster it will have kept track of those packages you manually installed, and will be able to mark as redundant those packages pulled in by dependencies alone which are no longer needed due to a package being removed. They will not mark for removal packages that you manually installed. To remove automatically installed packages that are no longer used, run:

  # apt autoremove

Do znalezienia zbędnych pakietów można również użyć programów deborphan, debfoster lub cruft. Nie należy usuwać wszystkich proponowanych przez to narzędzie pakietów bez zastanowienia (szczególnie, jeśli skorzysta się z agresywnych opcji, które nie są domyślne, a są podatne na nieprawidłowe wskazania). Powinno się osobiście przejrzeć pakiety sugerowane do usunięcia (ich zawartość, rozmiar i opis) przed ostateczną decyzją.


- Usunąć niepotrzebne tłumaczenia i pliki lokalizacji. Można zainstalować pakiet localepurge i skonfigurować go tak, aby zachował w systemie jedynie potrzebne tłumaczenia. Zredukuj to przestrzeń zajętą przez katalog /usr/share/locale.

- Tymczasowo przenieść na inny system lub usunąć całkowicie dzienniki systemowe z katalogu /var/log/.

- Użyć tymczasowego /var/cache/apt/archives; można użyć tymczasowego katalogu bufora z innego systemu plików (urządzenia USB, przenośnego dysku, używanego systemu plików, ...).

Proszę nie używać montowań NFS, ponieważ połączenie sieciowe może zostać przerwane przy aktualizacji.
Na przykład, jeśli napęd USB jest zamontowany w /media/usbkey:

1. usunięcie poprzednio pobranych pakietów do instalacji:

   ```bash
   # apt clean
   ```

2. skopiowanie katalogu /var/cache/apt/archives na napęd USB:

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

3. zamontowanie tymczasowego bufora w obecnym:

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

4. przywrócenie pierwotnego katalogu /var/cache/apt/archives po aktualizacji:

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

5. usunięcie pozostałego /media/usbkey/archives.

Tymczasowy bufor można utworzyć w dowolnym systemie plików zamontowanym w systemie.

- Wykonanie minimalnej aktualizacji (opisanej w Sekcja 4.4.4) lub częściowych aktualizacji systemu przed pełną aktualizacją. Umożliwi to częściową aktualizację systemu i pozwoli na wyczyszczenie bufora pakietów przed pełną aktualizacją.

Note that in order to safely remove packages, it is advisable to switch your APT source-list files back to buster as described in Sekcja A.2.

### 4.4.4 Minimalna aktualizacja systemu

**WAŻNE**

⚠️ If you are upgrading remotely, be aware of Sekcja 5.1.22.

W niektórych przypadkach bezpośrednie wykonanie pełnej aktualizacji (opisanej poniżej) może usuwać wiele pakietów które mają być zachowane. Z tego powodu zaleca się wykonanie dwustopniowej aktualizacji. Najpierw minimalnej, pozwalającej uporać się z tymi konfliktami, a następnie pełnej, zgodnie z opisem w Sekcja 4.4.5.

Aby to zrobić, proszę wykonać

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

W ten sposób aktualizowane zostaną pakiety, które nie wymagają usunięcia lub instalacji innych pakietów.

Minimalna aktualizacja systemu może okazać się przydatna również w systemach z niewielką ilością wolnego miejsca, na których pełna aktualizacja nie może być wykonana z tego powodu.

*If the apt-listchanges package is installed, it will (in its default configuration) show important information about upgraded packages in a pager after downloading the packages. Press q after reading to exit the pager and continue the upgrade.*
4.4.5 Aktualizacja systemu

Po wykonaniu poprzednich kroków, nadszedł czas na główną część aktualizacji. Proszę wykonać

```
# apt full-upgrade
```

Przeprowadzona zostanie w ten sposób pełna aktualizacja systemu, instalacja najnowszych dostępnych wersji wszystkich pakietów i rozwiązanie wszystkich możliwych zmian zależności pakietów w innych wydaniach. Jeśli jest to konieczne zainstalowane zostaną nowe pakiety (najczęściej nowe wersje bibliotek lub pakiety o nowych nazwach) i usunięte wszystkie niepotrzebne pakiety powodujące konflikty.

Przy aktualizacji z zestawu płyt CD/DVD/BD, użytkownik będzie prawdopodobnie proponowany włożenie określonej płyty w wielu miejscach aktualizacji. Z powodu zależności między pakietami rozproszonymi na poszczególnych nośnikach konieczne może okazać się wielokrotne wkładanie tej samej płyty.

New versions of currently installed packages that cannot be upgraded without changing the install status of another package will be left at their current version (displayed as „held back“). This can be resolved by either using aptitude to choose these packages for installation or by trying apt install package.

4.5 Możliwe problemy przy aktualizacji

Poniższe sekcje opisują znane problemy, które mogą pojawić się przy aktualizacji do wydania bullseye.

4.5.1 Podczas aktualizacji dystrybucji pojawia się błąd „Nie udało się wykonać natychmiastowej konfiguracji”.

In some cases the `apt full-upgrade` step can fail after downloading packages with:

```
E: Could not perform immediate configuration on ‘package’. Please see man 5 apt. ←
conf under APT::Immediate-Configure for details.
```

If that happens, running `apt full-upgrade -o APT::Immediate-Configure=0` instead should allow the upgrade to proceed.

Another possible workaround for this problem is to temporarily add both buster and bullseye sources to your APT source-list files and run `apt update`.

4.5.2 Spodziewane usunięcia pakietów


4.5.3 Konflikty lub pętle „wymaga wstępnio”

Sometimes it’s necessary to enable the APT::Force-LoopBreak option in APT to be able to temporarily remove an essential package due to a Conflicts/Pre-Depends loop. apt will alert you of this and abort the upgrade. You can work around this by specifying the option `-o APT::Force-LoopBreak=1` on the `apt` command line.

It is possible that a system’s dependency structure can be so corrupt as to require manual intervention. Usually this means using `apt` or

```
# dpkg --remove package_name
```

aby wyeliminować część przeszkadzających pakietów lub
ROZDZIAŁ 4. AKTUALIZACJA Z DEBIANA 10...

4.6. AKTUALIZACJA JĄDRA I POWIĄZANYCH...

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

W sytuacjach ekstremalnych konieczne może być wymuszenie reinstalacji za pomocą polecenia

```
# dpkg --install /path/to/package_name.deb
```

4.5.4 Konflikty plików

Konflikty plików nie powinny wystąpić przy aktualizacji z „czystego” wydania buster, lecz mogą się pojawić przy zainstalowanych nieoficjalnych backportach. Konflikty plików objawiają się komunikatami błędów, podobnymi do poniższego:

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

Można spróbować rozwiązać konflikt plików przez wymuszenie usunięcia pakietu wymienionego w ostatnim wierszu komunikatu błędu:

```
# dpkg -r --force-depends package_name
```

After fixing things up, you should be able to resume the upgrade by repeating the previously described `apt` commands.

4.5.5 Zmiany konfiguracji

Podczas aktualizacji zostaną wyświetlone pytania dotyczące konfiguracji lub ponownej konfiguracji kilku pakietów. Gdy pytanie będzie dotyczyło tego czy plik w katalogu `/etc/init.d` lub plik `/etc/manpath.config` ma zostać zastąpiony wersją opiekuna pakietu to odpowiedź powinna z regulą brzmieć „tak” (aby zapewnić spójność systemu). Zawsze można cofnąć się do starszej wersji, ponieważ są one zapisywane z rozszerzeniem `.dpkg-old`.

W razie wątpliwości, proszę zapisać nazwę pakietu lub pliku i zdecydować o tym później. Można przeszukać plik z zapisem sesji, aby znaleźć informację wyświetlaną na ekranie przy aktualizacji.

4.5.6 Zmiany sesji na konsoli

If you are running the upgrade using the system’s local console you might find that at some points during the upgrade the console is shifted over to a different view and you lose visibility of the upgrade process. For example, this may happen in systems with a graphical interface when the display manager is restarted.

Aby odzyskać konsole, na której trwa aktualizacja, należy wcisnąć Ctrl + Alt + F1, aby przełączyć się z powrotem na terminal wirtualny 1 z graficznego ekranu powitalnego lub Alt + F1 z trybu lokalnej konsoli tekstowej. Przesuń zastąpić F1 klawiszem funcyjnym o tym samym numerze co terminal wirtualny, na którym trwa aktualizacja. Można również skorzystać ze kombinacji Alt + strzałka w lewo lub Alt + strzałka w prawo aby przenosić się na kolejne terminaly tekstowe.

4.6 Aktualizacja jąдра i powiązanych pakietów

Niniejszy rozdział opisuje sposób aktualizacji jądra i identyfikacji potencjalnych problemów który mogą się pojawić. Można zainstalować jeden z pakietów `linux-image-*` udostępnionych przez Debiana lub skompilować dostosowany do swoich potrzeb.
ROZDZIAŁ 4. AKTUALIZACJA Z DEBIANA 10 ...

4.7. PRZYGOTOWANIE DO KOLEJNEGO ...

Proszę zauważyć, że wiele poniższych informacji zakłada, że używa się jednego z modularnych jąder Debiana razem z initramfs-tools i udev. Jeśli korzysta się z własnego, dostosowanego jądra, które nie wymaga initrd lub wykorzystuje się inny program tworzący initrd to część informacji będzie nieprzydatna.

4.6.1 Instalowanie metapakietu jądra

When you full-upgrade from buster to bullseye, it is strongly recommended that you install a linux-image-* metapackage, if you have not done so before. These metapackages will automatically pull in a newer version of the kernel during upgrades. You can verify whether you have one installed by running:

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

Jeśli nie zostanie wypisany żaden wynik potrzeba będzie albo zainstalować ręcznie nowy pakiet linux-image lub zainstalować metapakiet linux-image. Aby zobaczyć listę dostępnych metapakietów linux-image, proszę wykonać:

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

If you are unsure about which package to select, run `uname -r` and look for a package with a similar name. For example, if you see „4.9.0-8-amd64”, it is recommended that you install `linux-image-amd64`. You may also use `apt` to see a long description of each package in order to help choose the best one available. For example:

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

You should then use `apt install` to install it. Once this new kernel is installed you should reboot at the next available opportunity to get the benefits provided by the new kernel version. However, please have a look at Sekcja 5.1.24 before performing the first reboot after the upgrade.

For the more adventurous there is an easy way to compile your own custom kernel on Debian. Install the kernel sources, provided in the `linux-source` package. You can make use of the `deb-pkg` target available in the sources' makefile for building a binary package. More information can be found in the Debian Linux Kernel Handbook (https://kernel-team.pages.debian.net/kernel-handbook/), which can also be found as the debian-kernel-handbook package.

If possible, it is to your advantage to upgrade the kernel package separately from the main full-upgrade to reduce the chances of a temporarily non-bootable system. Note that this should only be done after the minimal upgrade process described in Sekcja 4.4.4.

4.7 Przygotowanie do kolejnego wydania

Po aktualizacji jest kilka rzeczy, które można zrobić w celu przygotowania do następnego wydania.


4.7.1 Czyszczenie usuniętych pakietów

Ogólnym zaleceniem jest czyszczenie usuniętych pakietów. Ma to szczególny sens, jeśli pakiety zostały usunięte we wcześniejszej aktualizacji wydania (np. przy aktualizacji do buster) lub pochodzą od zewnętrznych dostawców. W szczególności znane są problemy ze starymi skryptami init.d.
4.8 Przestarzałe pakiety

Wprowadzając wiele nowych pakietów, bullseye porzuca i pomija również sporę starych pakietów z wydania buster. Nie ma dla nich ścieżki aktualizacji. Choć nic nie stoi na przeszkodzie, aby w razie potrzeby używać takich pakietów to projekt Debian kończy wsparcie bezpieczeństwa po roku od wydania bullseye\(^5\) i nie dostarcza innego wsparcie w międzyczasie. Zaleca się zastąpienie ich dostępnymi alternatywami jeśli takie istnieją.

Jest wiele powodów, dla których pakiet mógł zostać usunięty z dystrybucji: nie jest dłużej utrzymany przez projekt macierzysty, nie ma chętnego Dewelopera Debiana, który byłby zainteresowany opiekowaniem się pakietem, funkcja którą pełnił została przejęta przez inne programy (lub nowszą wersję), nie jest dłużej uważany za odpowiedni dla wydania bullseye ze względu na poważne błędy. W tym ostatnim przypadku pakiet może być wciąż obecny w dystrybucji „niestabilnej”.

Some package management front-ends provide easy ways of finding installed packages that are no longer available from any known repository. The \texttt{aptitude} textual user interface lists them in the category „Obsolete and Locally Created Packages”, and they can be listed and purged from the commandline with:

\begin{verbatim}
# aptitude search ‘~o’
# aptitude purge ‘~o’
\end{verbatim}


Lista pakietów uznanych za przestarzałe w wydaniu Bullseye jest dostępna w: Sekcja 5.3.1.

4.8.1 Transitional dummy packages

Some packages from buster may have been replaced in bullseye by transitional dummy packages, which are empty placeholders designed to simplify upgrades. If for instance an application that was formerly a single package has been split into several, a transitional package may be provided with the same name

\(^5\)Lub tak długo, aż nie pojawi się nowe wydanie w tym czasie. Zwykle jedynie dwa wydania stabilne są wspierane w dowolnym czasie.
as the old package and with appropriate dependencies to cause the new ones to be installed. After this has happened the redundant dummy package can be safely removed.

The package descriptions for transitional dummy packages usually indicate their purpose. However, they are not uniform; in particular, some „dummy” packages are designed to be kept installed, in order to pull in a full software suite, or track the current latest version of some program. You might also find deborphan with the --guess-* options (e.g. --guess-dummy) useful to detect transitional dummy packages on your system.
Rozdział 5

Problem, które należy mieć na uwadze, a dotyczące wydania bullseye

Czasami zmiany wprowadzone w nowym wydaniu mają skutki uboczne, którym nie można zapobiec w sensowny sposób, lub które odsłaniają inne błędy. Niniejszy rozdział dokumentuje znane problemy. Proszę zapoznać się również z erratą, dokumentacją odpowiednich pakietów, zgłoszeniami błędów i pozostałymi informacjami opisanymi w Sekcja 6.1.

5.1 Uwagi dotyczące aktualizacji do bullseye

Niniejszy rozdział dotyczy aktualizacji z wydania buster do bullseye.

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

### 5.1.7 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 cgroupr2 by default (see Sekcja 2.2.4), the sysfs tree in /sys/fs/cgroup will not include cgroup v1 features such as /sys/fs/cgroupblkio, 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 Sekcja 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 Rozdział 4, packages depending on fuse3 might be kept back during upgrades. Running the steps discussed in Sekcja 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_userns_clone=0 has a similar effect, but is deprecated.

5.1.14 Linux disables unprivileged calls to bpf() by default

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

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

```
kernnel.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 redminemissinginbullseye

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

5.1.16 Exim 4.94

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

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

Typical nonworking examples include:

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

Using

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

instead of

```plaintext
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

```plaintext
.ifdef _GPT_MAIN_ALLOW_INSECURE_TAINTED_DATA
allow_insecure_tainted_data = yes
.endif
```

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

5.1.17 SCSI device probing is non-deterministic

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

5.1.18 rdiff-backup require lockstep upgrade of server and client

The network protocol of versions 1 and 2 of rdiff-backup are incompatible. This means that you must be running the same version (either 1 or 2) of rdiff-backup locally and remotely. Since buster ships version 1.2.8 and bullseye ships version 2.0.5, upgrading only the local system or only the remote system from buster to bullseye will break rdiff-backup runs between the two.
Version 2.0.5 of rdiff-backup is available in the buster-backports archive, see backports (https://backports.debian.org/). This enables users to first upgrade only the rdiff-backup package on their buster systems, and then independently upgrade systems to bullseye at their convenience.

### 5.1.19 Intel CPU microcode issues

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

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

### 5.1.20 Upgrades involving libgc1c2 need two runs

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

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

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

### 5.1.22 No new SSH connections possible during upgrade

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

### 5.1.23 Open vSwitch upgrade requires interfaces(5) change

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

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

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

### 5.1.24 Sprawy do zrobienia przed ponownym uruchomieniem

When apt full-upgrade has finished, the „formal” upgrade is complete. For the upgrade to bullseye, there are no special actions needed before performing a reboot.
5.2 Items not limited to the upgrade process

5.2.1 Ograniczenia we wsparciu bezpieczeństwa

Istnieje kilka pakietów, którym Debian nie może zapewnić minimalnego wsparcia bezpieczeństwa. Szczegółowo opisano je poniżej.

**NOTATKA**

The package `debian-security-support` helps to track the security support status of installed packages.

5.2.1.1 Security status of web browsers and their rendering engines

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

For general web browser use we recommend Firefox or Chromium. They will be kept up-to-date by rebuilding the current ESR releases for stable. The same strategy will be applied for Thunderbird.

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 Accessing GNOME Settings app without mouse

Without a pointing device, there is no direct way to change settings in the GNOME Settings app provided by `gnome-control-center`. As a work-around, you can navigate from the sidebar to the main content by pressing the Right Arrow twice. To get back to the sidebar, you can start a search with Ctrl+F, type something, then hit Esc to cancel the search. Now you can use the Up Arrow and Down Arrow to navigate the sidebar. It is not possible to select search results with the keyboard.

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

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).

5.3 Obsolescence and deprecation

5.3.1 Znane pakiety oznaczone jako przestarzałe

Poniższa lista zawiera znane i warte uwagi pakiety, które zostały uznane za przestarzałe (zob. wyjaśnienie w Sekcja 4.8).

Lista przestarzałych pakietów obejmuje:

- 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 `isdntools`, `isdncard`, `drd6l` 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).

- 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.
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:

<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 MA-ILTO causes breakage</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>991081</td>
<td>gir1.2-diodon-1.0</td>
<td>gir1.2-diodon-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;= 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 exfatprogs and backport the commit that rejects exfat-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 untitled 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>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>
</tbody>
</table>
### 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>991151</td>
<td>procps</td>
<td>procps: 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:gemu</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>
<tr>
<td>991822</td>
<td>src:wine</td>
<td>src:wine: dh_auto_clean deletes unrelated files outside of package source</td>
</tr>
<tr>
<td>988477</td>
<td>src:xen</td>
<td>xen-hypervisor-4.14-amd64: xen dmesg shows (XEN) AMD-Vi: IO PAGE_FAULT on sata pci device</td>
</tr>
<tr>
<td>991788</td>
<td>xfce4-settings</td>
<td>xfce4-settings: black screen after suspend when laptop lid is closed and re-opened</td>
</tr>
</tbody>
</table>
Rozdział 6

Więcej informacji na temat projektu Debian

6.1 Dodatkowe informacje


Dokumentacja poszczególnych pakietów jest instalowana do katalogów /usr/share/doc/pakiet. Mogą być to informacje o prawach autorskich, detale dystrybucji Debian lub dokumentacja z projektu macierzystego.

6.2 Pomoc

Istnieje wiele źródeł pomocy, rady i wsparcia dla użytkowników Debiana, lecz powinno się z nich korzystać dopiero wtedy, gdy przeszukało się dostępną dokumentację, która mogła zawierać wyjaśnienie problemu. Niniejszy rozdział jest krótkim wprowadzeniem który może okazać się pomocny dla nowych użytkowników Debiana.

6.2.1 Listy dyskusyjne


6.2.2 IRC

Debian ma kanał IRC, który jest przeznaczony do pomocy użytkownikom Debiana (w sieci IRC OFTC). Dostęp do kanału można uzyskać ze swojego klienta IRC, pod adresem irc.debian.org, wybierając kanał #debian. Obowiązującym językiem jest angielski.


Więcej informacji o OFTC można znaleźć na odpowiedniej stronie internetowej (http://www.oftc.net/).
6.3 Zgłaszanie błędów

Staramy się, aby Debian był systemem operacyjnym wysokiej jakości, jednak nie znaczy to, że udostępniane pakiety są całkowicie wolne od błędów. Zgodnie z filozofią „otwartego rozwoju” Debiana oraz jako usługa dla naszych użytkowników, dostarczamy wszystkie informacje o zgłoszonych błędach w naszym Systemie Śledzenia Błędów (Bug Tracking System - BTS). BTS można przeglądać pod adresem https://bugs.debian.org/.

W przypadku znalezienia błędu w dystrybucji lub spakowanym programie będącym jej częścią prosimy o zgłoszenie błędu, dzięki czemu będzie mógł zostać poprawiony w kolejnych wydaniach. Zgłaszanie błędów wymaga poprawnego adresu poczty elektronicznej. Dzięki niemu możliwe jest śledzenie błędów i kontakt deweloperów ze zgłaszającym, w razie potrzeby uzyskania dodatkowych informacji.

Błędy można zgłaszać za pomocą programu reportbug lub ręcznie, za pomocą poczty elektronicznej. Więcej informacji o Systemie Śledzenia Błędów i sposobie korzystania z niego, zawiera dokumentacja (dostępna w /usr/share/doc/debian, jeśli zainstalowano pakiet doc-debian) lub strona System Śledzenia Błędów (https://bugs.debian.org/).

6.4 Uczestnictwo w rozwoju Debiana

You do not need to be an expert to contribute to Debian. By assisting users with problems on the various user support lists (https://lists.debian.org/) you are contributing to the community. Identifying (and also solving) problems related to the development of the distribution by participating on the development lists (https://lists.debian.org/) is also extremely helpful. To maintain Debian’s high-quality distribution, submit bugs (https://bugs.debian.org/) and help developers track them down and fix them. The tool how-can-i-help helps you to find suitable reported bugs to work on. If you have a way with words then you may want to contribute more actively by helping to write documentation (https://www.debian.org/doc/vcs) or translate (https://www.debian.org/international/) existing documentation into your own language.


W każdym razie, niezaleźnie od tego, czy działa się na rzecz społeczności Wolnego Oprogramowania jako użytkownik, programista, osoba zajmująca się pisaniem dokumentacji lub tłumaczeniami, już teraz dokłada się swoją cegiełkę w budowie Wolnego Oprogramowania. Taka praca daje dużo satysfakcji i radości oraz pozwala na poznanie nowych ludzi.
Rozdział 7

Glossary

ACPI
Advanced Configuration and Power Interface

ALSA
Advanced Linux Sound Architecture (zaawansowana architektura dźwięku Linuksa)

BD
Blu-ray Disc

CD
Compact Disc

CD-ROM
Compact Disc Read Only Memory

DHCP
Dynamic Host Configuration Protocol

DLBD
Dual Layer Blu-ray Disc (dwuwarstwowa płyta Blu-ray)

DNS
Domain Name System

DVD
Digital Versatile Disc

GIMP
GNU Image Manipulation Program

GNU
GNU’s Not Unix (GNU to nie Unix)

GPG
GNU Privacy Guard

LDAP
Lightweight Directory Access Protocol

LSB
Linux Standard Base

LVM
Logical Volume Manager

MTA
Mail Transport Agent
NBD
Network Block Device

NFS
Network File System (sieciowy system plików)

NIC
Network Interface Card

NIS
Network Information Service

PHP
PHP: Hypertext Preprocessor

RAID
Redundant Array of Independent Disks

SATA
Serial Advanced Technology Attachment

SSL
Secure Sockets Layer

TLS
Transport Layer Security

UEFI
Unified Extensible Firmware Interface

USB
Universal Serial Bus (uniwersalna magistrala szeregowa)

UUID
Universally Unique Identifier

WPA
Wi-Fi Protected Access
Dodatek A

Zarządzanie wydaniem buster przed aktualizacją

Dodatek zawiera informacje pozwalające upewnić się, że można instalować lub aktualizować pakiety z buster przed aktualizacją do bullseye. Jest to konieczne tylko w szczególnych przypadkach.

A.1 Uaktualnienie wydania buster

Nie różni się to od żadnej innej aktualizacji, którą przeprowadzano wcześniej w wydaniu buster. Jedyną różnicą jest konieczność upewnienia się, że lista pakietów wciąż odnosi się do buster, tak jak wyjaśniono to w Sekcja A.2.

Przy aktualizowaniu systemu z serwera lustrzanego Debiana, zostanie on automatycznie uaktualniony do ostatniego wydania punktowego buster.

A.2 Checking your APT source-list files

If any of the lines in your APT source-list files (see sources.list(5) (https://manpages.debian.org/bullseye/apt/sources.list.5.html)) contain references to „stable”, this is effectively pointing to bullseye already. This might not be what you want if you are not yet ready for the upgrade. If you have already run apt update, you can still get back without problems by following the procedure below.

Jeśli zainstalowało się już pakiety z wydania bullseye, to prawdopodobnie nie ma sensu instalowania pakietów ze starego wydania buster. Proszę wówczas zdecydować czy chce się kontynuować czy też nie. Instalowanie starszych wersji pakietów jest technicznie możliwe lecz nie zostało tu opisane.

As root, open the relevant APT source-list file (such as /etc/apt/sources.list) with your favorite editor, and check all lines beginning with deb http:, deb https:, deb tor+http:, deb tor+https:, URIs: http:, URIs: https:, URIs: tor+http: or URIs: tor+https: for a reference to „stable”. If you find any, change stable to buster.

If you have any lines starting with deb file: or URIs: file:, you will have to check for yourself if the location they refer to contains a buster or bullseye archive.

WAŻNE

Do not change any lines that begin with deb cdrom: or URIs: cdrom: Doing so would invalidate the line and you would have to run apt-cdrom again. Do not be alarmed if a cdrom: source line refers to „unstable”. Although confusing, this is normal.

Jeśli dokonało się jakichś zmian, proszę zapisać plik i wykonać
A.3 Usunięcie przestarzałych plików konfiguracyjnych

Przed aktualizacją do bullseye, zaleca się usunąć stare pliki konfiguracyjne (takie jak *.dpkg-{new, old} z /etc.

```bash
# apt update

aby odświeżyć listę pakietów.
```
Dodatek B

Współtwórcy uwag do wydania

W tworzeniu uwag do wydania brało udział wiele osób, między innymi

Niniejszy dokument został przetłumaczony na wiele języków. Podziękowania dla wszystkich tłumaczy!

Indeks

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, 3
GnuPG, 4

I
Inkscape, 4

K
KDE, 3

L
LibreOffice, 3
LXDE, 3
LXQt, 3

M
MariaDB, 4
MATE, 3

N
Nginx, 4

O
OpenJDK, 4
OpenSSH, 4

P
packages
apt, 2, 14, 27
apt-listchanges, 18
aptitude, 12, 17, 22
aufs-dkms, 32
bsd-mailx, 29
cacertificates-java, 32
chef, 31
cinder-volume, 26
connm, 32
cron, 32
cups-browsed, 4
cups-daemon, 4
cups-filters, 4
dblatex, 2
debian-goodies, 17
debian-kernel-handbook, 21
debian-security-support, 30
doc-debian, 36
docbook-xsl, 2
dpkg, 2
drdsl, 31
exfat-fuse, 5
exfat-utils, 6
exfatprogs, 6
fail2ban, 29, 33
firmware-iwlwifi, 29
fuse, 27
fuse3, 27
gcc-10-base, 33
gir1.2-diodon-1.0, 33
gir1.2-gtd-1.0, 33
git-el, 33
glibc, 26
gnome-control-center, 30
gparted, 33
grub2, 31
guile-2.2-libs, 29
gvfs-fuse, 27
how-can-i-help, 36
ibod, 31
ifenslave, 33
initramfs-tools, 10, 21
intel-microcode, 29
ipp-usb, 4, 5
isdnactivecards, 31
isdnutils, 31
kio-fuse, 27
libappindicator-dev, 31
libappindicator1, 31
libappindicator3-1, 31
libbatatana-appindicator, 31
libgc1c2, 29
libjs-bootstrap4, 34
libnss-nis, 26
libnss-nisplus, 26
libpam-chroot, 33
libpython3.9-dev, 34
libsane1, 4, 5
lilo, 31
linux-image-*, 20
linux-image-amd64, 21
linux-source, 21
localepurge, 17
mailman, 31
mailman3, 31
mailman3-full, 31
mailutils, 29
mariadb-server-10.5,galera-4, 33
mdadm, 33
network-manager, 32
nova-compute, 26
openipmi, 33
openssh-server, 29, 33
openvswitch, 29
popularity-contest, 17
procp, 34
pulseaudio, 34
python-pkg-resources, 33
python-setuptools, 31
rails, 28
rdiff-backup, 28, 29
redmine, 28
release-notes, 1
rsync, 26
rsyslog, 5
sane-airscan, 4
sendmail, 27
slapd, 32
speech-dispatcher, 34
src:gcc-10, 33
src:llvm-toolchain-11, 33
src:qemu, 34
src:squid-deb-proxy, 34
src:wine, 34
src:xen, 34
sshfs, 27
synaptic, 12
systemd, 6
tinc, 11
tpm2-abrmd, 34
udev, 21, 28
unbound, 26
upgrade-reports, 1
usrmerge, 32
vim, 26
vim-addon-manager, 26
vim-scripts, 26
wicd, 32
xfce4-settings, 34
xmlroff, 2
xsltproc, 2
Perl, 4
PHP, 4
Postfix, 4
PostgreSQL, 4

X
Xfce, 3