

# **Uwagi do wydania, do dystrybucji Debian 11 (bullseye), 64-bitowe PC**

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

26 czerwca 2022

---

## Uwagi do wydania, do dystrybucji Debian 11 (bullseye), 64-bitowe PC

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.

# Spis treści

<b>1</b>	<b>Wstęp</b>	<b>1</b>
1.1	Zgłaszanie błędów w tym dokumencie	1
1.2	Wysyłanie sprawozdań aktualizacji	1
1.3	Źródła niniejszego dokumentu	2
<b>2</b>	<b>Nowości w dystrybucji Debian 11</b>	<b>3</b>
2.1	Obsługiwane architektury	3
2.2	Co nowego w dystrybucji?	3
2.2.1	Desktops and well known packages	3
2.2.2	Driverless scanning and printing	4
2.2.2.1	CUPS and driverless printing	4
2.2.2.2	SANE and driverless scanning	4
2.2.3	New generic open command	5
2.2.4	Control groups v2	5
2.2.5	Persistent systemd journal	5
2.2.6	New Fcitx 5 Input Method	5
2.2.7	Więści z odmiany Debian Med	5
2.2.8	Kernel support for exFAT	5
2.2.9	Improved man page translations	6
2.2.10	Improved support for alternative init systems	6
<b>3</b>	<b>System instalacyjny</b>	<b>7</b>
3.1	Co nowego w systemie instalacyjnym?	7
3.1.1	Help with installation of firmware	7
3.1.2	Instalacja automatyczna	7
3.2	Cloud installations	8
3.3	Container and Virtual Machine images	8
<b>4</b>	<b>Aktualizacja z Debiana 10 (buster)</b>	<b>9</b>
4.1	Przygotowanie do aktualizacji	9
4.1.1	Kopia zapasowa danych i konfiguracji	9
4.1.2	Upřednie ostrzeżenie użytkowników	9
4.1.3	Przygotowanie do przestoju usług	9
4.1.4	Przygotowanie do odzyskiwania	10
4.1.4.1	Debugowanie powłoki podczas rozruchu przy użyciu initrd	10
4.1.4.2	Debugowanie powłoki podczas rozruchu przy użyciu systemd	10
4.1.5	Przygotowanie bezpiecznego środowiska do uaktualnienia	11
4.2	Start from „pure” Debian	11
4.2.1	Upgrade to Debian 10 (buster)	11
4.2.2	Remove non-Debian packages	11
4.2.3	Upgrade to latest point release	12
4.2.4	Prepare the package database	12
4.2.5	Remove obsolete packages	12
4.2.6	Clean up leftover configuration files	12
4.2.7	The security section	12
4.2.8	Sekcja proposed-updates	12
4.2.9	Nieoficjalne źródła	12
4.2.10	Wyłączenie priorytetów APT-a (APT pinning)	12
4.2.11	Check package status	13
4.3	Preparing APT source-list files	13
4.3.1	Dodanie internetowych źródeł APT-a	14
4.3.2	Dodanie źródeł APT-a do lokalnego serwera lustrzanego	14
4.3.3	Dodanie źródeł APT-a do nośników optycznych	15
4.4	Aktualizacja pakietów	15

---

4.4.1	Zapisanie sesji	15
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 natychmiastowej 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	21
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
<b>5</b>	<b>Problemy, które należy mieć na uwadze, a dotyczące wydania bullseye</b>	<b>25</b>
5.1	Uwagi dotyczące aktualizacji do bullseye	25
5.1.1	New VA-API default driver for Intel GPUs	25
5.1.2	The XFS file system no longer supports barrier/nobarrier option	25
5.1.3	Changed security archive layout	25
5.1.4	Password hashing uses yescrypt by default	26
5.1.5	NSS NIS and NIS+ support require new packages	26
5.1.6	Config file fragment handling in unbound	26
5.1.7	rsync parameter deprecation	26
5.1.8	Vim addons handling	26
5.1.9	OpenStack and cgroups v1	26
5.1.10	OpenStack API policy files	27
5.1.11	sendmail downtime during upgrade	27
5.1.12	FUSE 3	27
5.1.13	GnuPG options file	27
5.1.14	Linux enables user namespaces by default	27
5.1.15	Linux disables unprivileged calls to bpf() by default	27
5.1.16	redmine missing in bullseye	28
5.1.17	Exim 4.94	28
5.1.18	SCSI device probing is non-deterministic	28
5.1.19	rdiff-backup require lockstep upgrade of server and client	29
5.1.20	Intel CPU microcode issues	29
5.1.21	Upgrades involving libgc1c2 need two runs	29
5.1.22	fail2ban can't send e-mail using mail from BSD-mailx	29
5.1.23	No new SSH connections possible during upgrade	29
5.1.24	Open vSwitch upgrade requires interfaces(5) change	29
5.1.25	Sprawy do zrobienia przed ponownym uruchomieniem	30
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 pakiety oznaczone jako przestarzałe	31
5.3.2	Przestarzałe składniki w wydaniu bullseye	32
5.4	Known severe bugs	32

---

<b>6</b>	<b>Więcej informacji na temat projektu Debian</b>	<b>35</b>
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
<b>7</b>	<b>Glossary</b>	<b>37</b>
<b>A</b>	<b>Zarządzanie wydaniem buster przed aktualizacją</b>	<b>39</b>
A.1	Uaktualnienie wydania buster . . . . .	39
A.2	Checking your APT source-list files . . . . .	39
A.3	Usunięcie przestarzałych plików konfiguracyjnych . . . . .	40
<b>B</b>	<b>Współtwórcy uwag do wydania</b>	<b>41</b>
	<b>Indeks</b>	<b>43</b>



# 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>.

### 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 Debiana (buster). W przypadku aktualizacji ze starszych wydań, sugerujemy uprzednie zapoznanie się z poprzednią wersją informacji o wydaniu i aktualizację do Debiana 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/) (<https://bugs.debian.org/>) wobec pakietu `release-notes` (w języku angielskim). Wcześniej można przejrzeć [listę zauważonych błędów](https://bugs.debian.org/release-notes) (<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 przysyłać na polskojęzyczną listę `debian-l10n-polish`.

Cenimy i zalecamy zgłaszanie łątek do źródeł tego dokumentu. Więcej informacji o pobieraniu ich można znaleźć w Sekcja [1.3](#).

## 1.2 Wysyłanie sprawozdań aktualizacji

Z chęcią przyjmimy każdą informację (w języku angielskim) dotyczącą aktualizacji z wydania buster do bullseye. Aby przesłać te informacje, proszę zgłosić błąd w [systemie śledzenia błędów](https://bugs.debian.org/) (<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:

- 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 Sekcją 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/) (<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) (<https://www.debian.org/doc/vcs>).



## Rozdział 2

# Nowości w dystrybucji Debian 11

The [Wiki](https://wiki.debian.org/NewInBullseye) (<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/) (<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;

Poza wieloma innymi, to wydanie zawiera następujące aktualizacje oprogramowania:

Pakiet	Wersja w 10 (buster)	Wersja w 11 (bullseye)
Apache	2.4.38	2.4.48
Serwer DNS BIND	9.11	9.16
Cryptsetup	2.1	2.3
Dovecot MTA	2.3.4	2.3.13
Emacs	26.1	27.1
Domyślny serwer pocztowy Exim	4.92	4.94
GNU Compiler Collection jako domyślny kompilator	8.3	10.2
GIMP	2.10.8	2.10.22
GnuPG	2.2.12	2.2.27
Inkscape	0.92.4	1.0.2
Biblioteka C GNU	2.28	2.31
lighttpd	1.4.53	1.4.59
Obraz jądra Linux	4.19 series	5.10 series
LLVM/Clang toolchain	6.0.1 and 7.0.1 (default)	9.0.1 and 11.0.1 (default)
MariaDB	10.3	10.5
Nginx	1.14	1.18
OpenJDK	11	11
OpenSSH	7.9p1	8.4p1
Perl	5.28	5.32
PHP	7.3	7.4
Postfix MTA	3.4	3.5
PostgreSQL	11	13
Python 3	3.7.3	3.9.1
Rustc	1.41 (1.34 for armel)	1.48
Samba	4.9	4.13
Vim	8.1	8.2

## 2.2.2 Driverless scanning and printing

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

### 2.2.2.1 CUPS and driverless printing

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

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

### 2.2.2.2 SANE and driverless scanning

The official SANE driverless backend is provided by `sane-escl` in `libsane1`. An independently developed driverless backend is `sane-airscan`. Both backends understand the **eSCL protocol** (<https://wiki.debian.org/SaneOverNetwork#escl>) but `sane-airscan` can also use the **WSD** (<https://wiki.debian.org/SaneOverNetwork#wsd>) protocol. Users should consider having both backends on their systems.

eSCL and WSD are network protocols. Consequently they will operate over a USB connection if the device is an `IPP-over-USB` device (see above). Note that `libsane1` has `ipp-usb` as a recommended package. This leads to a suitable device being automatically set up to use a driverless backend driver when it is connected to a USB port.

### 2.2.3 New generic open command

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

### 2.2.4 Control groups v2

In bullseye, `systemd` defaults to using control groups v2 (`cgroupv2`), which provides a unified resource-control hierarchy. Kernel commandline parameters are available to re-enable the legacy `cgroups` if necessary; see the notes for OpenStack in Sekcja 5.1.9 section.

### 2.2.5 Persistent systemd journal

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

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

### 2.2.6 New Fcix 5 Input Method

Fcix 5 is an input method for Chinese, Japanese, Korean and many other languages. It is the successor of the popular Fcix 4 in buster. The new version supports Wayland and has better addon support. More information including the migration guide can be found **on the wiki** (<https://wiki.debian.org/I18n/Fcix5>).

### 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** (<https://wiki.debian.org/SIMDEverywhere>). This library allows packages to be available on more hardware platforms supported by Debian (notably on `arm64`) while maintaining the performance benefit brought by processors supporting vector extensions, such as `AVX` on `amd64`, or `NEON` on `arm64`.

To install packages maintained by the Debian Med team, install the metapackages named `med-*`, which are at version 3.6.x for Debian bullseye. Feel free to visit the **Debian Med tasks pages** (<https://blends.debian.org/med/tasks>) to see the full range of biological and medical software available in Debian.

### 2.2.8 Kernel support for exFAT

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

continue to use the filesystem-in-userspace implementation, you need to invoke the `mount.exfat-fuse` helper directly when mounting an exFAT filesystem.

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

### 2.2.9 Improved man page translations

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

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

### 2.2.10 Improved support for alternative init systems

The default init system in Debian is `systemd`. In bullseye, a number of alternative init systems are supported (such as System-V-style `init` and `OpenRC`), and most desktop environments now work well on systems running alternative inits. Details on how to switch init system (and where to get help with issues related to running inits other than `systemd`) are available [on the Debian wiki](https://wiki.debian.org/Init) (<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 są 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/) (<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 [erratą](https://www.debian.org/releases/bullseye/debian-installer/index#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/) (<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](https://www.debian.org/releases/bullseye/debian-installer/#firmware_nonfree) ([https://www.debian.org/releases/bullseye/debian-installer/#firmware\\_nonfree](https://www.debian.org/releases/bullseye/debian-installer/#firmware_nonfree))). The firmware is usually not DFSG compliant, so it is not possible to distribute it in Debian's main repository.

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

#### 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.

[Przewodnik po instalacji](https://www.debian.org/releases/bullseye/installmanual) (<https://www.debian.org/releases/bullseye/installmanual>) zawiera zaktualizowany dodatek opisujący szczegółowo używanie wstępnej konfiguracji.

## 3.2 Cloud installations

The **cloud team** (<https://wiki.debian.org/Teams/Cloud>) publishes Debian bullseye for several popular cloud computing services including:

- OpenStack
- Amazon Web Services
- Microsoft Azure

Cloud images provide automation hooks via cloud-init and prioritize fast instance startup using specifically optimized kernel packages and grub configurations. Images supporting different architectures are provided where appropriate and the cloud team endeavors to support all features offered by the cloud service.

The cloud team will provide updated images until the end of the LTS period for bullseye. New images are typically released for each point release and after security fixes for critical packages. The cloud team's full support policy can be found [here](https://wiki.debian.org/Cloud/ImageLifecycle) (<https://wiki.debian.org/Cloud/ImageLifecycle>).

More details are available at [cloud.debian.org](https://cloud.debian.org/) (<https://cloud.debian.org/>) and [on the wiki](https://wiki.debian.org/Cloud/) (<https://wiki.debian.org/Cloud/>).

## 3.3 Container and Virtual Machine images

Multi-architecture Debian bullseye container images are available on [Docker Hub](https://hub.docker.com/_/debian) ([https://hub.docker.com/\\_/debian](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) (<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 sprzętowy w trakcie procedury może spowodować znaczne uszkodzenie systemu.

Główną rzeczą, którą warto skopiować jest zawartość plików `/etc`, `/var/lib/dpkg`, `/var/lib/apt/extended_states` oraz wynik polecenia `dpkg --get-selections "*" (cudzysłów jest istotny)`. Jeśli do zarządzania pakietami wykorzystuje się program **aptitude**, należy zachować również zawartość pliku `/var/lib/aptitude/pkgstates`.

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 domyślnymi, gdy użytkownik uruchamia dany program jako pierwszy. Środkiem ostrożności jest wykonanie kopii zapasowych ukrytych plików i katalogów (z kropką - „dotfiles”) z katalogów domowych użytkowników. Ta kopia może ułatwić odtworzenie 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 Upřednie 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 przestoju 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.

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 niedostępnych<sup>1</sup> w dłuższym okresie.

Jeśli aktualizowany system udostępnia usługi, które są krytyczne dla użytkowników bądź sieci<sup>2</sup>, można ograniczyć przerwę w ich działaniu wykonując aktualizację minimalną (zgodnie z opisem w Sekcja 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 Sekcja 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 uruchomił 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 uruchomi się on po aktualizacji (lub w przypadku systemów zarządzanych zdalnie nie zaktywuje 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.

W sytuacjach awaryjnych zalecamy użycie *trybu ratunkowego* w instalatorze Debiana bullseye. Zalecą skorzystania z instalatora jest możliwość wyboru takiej metody jaka jest najkorzystniejsza. Więcej informacji zawiera „Recovering a Broken System” w rozdziale 8 *przewodnika instalacji* (<https://www.debian.org/releases/bullseye/installmanual>) i *FAQ instalatora Debiana* (<https://wiki.debian.org/DebianInstaller/FAQ>).

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 debugowania<sup>3</sup> w generowanych obrazach `initrd`. Na przykład: jeśli `initrd` nie będzie mógł zamontować głównego systemu plików to przeniesie się do powłoki debugowania z dostępnymi podstawowymi poleceniami, 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. Wynik `dmesg` pokaże również jakie pliki urządzeń zostały przypisane do danych dysków; powinno się je 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 korzystając 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`.

<sup>1</sup>Jeśli priorytet `debconfa` jest ustawiony na bardzo wysoką wartość, to może to spowodować niewyświetlanie pytań konfiguracyjnych. Usługi zależne od domyślnych odpowiedzi, które nie będą pasowały do danego systemu, nie uruchomią się.

<sup>2</sup>Przykład: usługi DNS i DHCP, szczególnie jeśli nie ma redundancji lub tzw. failover. W przypadku DHCP użytkownicy mogą zostać odłączeni z sieci, jeśli czas dzierżawy jest mniejszy niż czas trwania aktualizacji.

<sup>3</sup>Można wyłączyć tę funkcję dodając parametr `panic=0` do parametrów rozruchowych.



Z kolei parametr jądra `systemd.unit=emergency.target` udostępni powłokę roota najwcześniej 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/) (<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) (<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) (<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 5.1.3.

### 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 plików<sup>4</sup>. 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) ([https://manpages.debian.org//bullseye/apt/apt\\_preferences.5.en.html](https://manpages.debian.org//bullseye/apt/apt_preferences.5.en.html)).

<sup>4</sup>System 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
```

Pożądanym 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 wydaniem Debiana:

- By [subscribing to the Debian announcement mailing list](https://lists.debian.org/debian-announce) (<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`.

- Po zapisaniu się do listy dyskusyjnej z ogłoszeniami związanymi z bezpieczeństwem Debiana (<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).

Żałujemy 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-amd64/...
http://mirrors.kernel.org/debian/dists/bullseye/contrib/binary-amd64/...
```

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-amd64/...
/var/local/debian/dists/bullseye/contrib/binary-amd64/...
```

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 wykonać

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

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 i `/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:

```
# script -t 2>~/upgrade-bullseyestep.time -a ~/upgrade-bullseyestep.script
```

lub coś podobnego. Jeśli będzie trzeba uruchomić zapis ponownie (np. po ponownym uruchomieniu systemu), proszę użyć innej wartości *krok*, aby wskazać zapisywany 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 restarcie.

Zapis ten pozwoli również na przejrzenie 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 przejrzeć 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 odtworzyć całą sesję:

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

## NOTATKA



Wykonanie tego polecenia na początku procesu aktualizacji może wypisać błąd, z powodów opisanych w następnych rozdziałach. Trzeba wówczas poczekać z komendą do zakończenia minimalnej aktualizacji systemu (opisanej w Sekcja 4.4.4)

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 pakiety zajmujące zbyt dużo miejsca, które nie są obecnie potrzebne (można je zawsze doinstalować po aktualizacji). Jeśli zainstalowano pakiet `popularity-contest` to do wyświetlenia listy nieużywanych pakietów zajmujących najwięcej miejsca można posłużyć się poleceniem **popcon-largest-unused**. Największe pakiety można znaleźć poleceniem **dpigs** (z pakietu `debian-goodies`) lub programem **wajig** (poleceniem `wajig size`). Można użyć także programu **aptitude**. W tym celu proszę uruchomić **aptitude** w graficznym interfejsie terminalowym, wybrać Widoki → Nowy płaski widok pakietów, wcisnąć **l**, wpisać `~i`, następnie wcisnąć **S** i wpisać `~installsize`. W ten sposób można otrzymać zwięzłą listę do dalszych działań.
- Usunąć niepotrzebne tłumaczenia i pliki lokalizacji. Można zainstalować pakiet `localepurge` i skonfigurować go tak, aby zachował w systemie jedynie potrzebne tłumaczenia. Zredukuje 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, ...).

## NOTATKA



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:

```
# apt clean
```

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

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

3. zamontowanie tymczasowego bufora w obecnym:

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

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

```
# 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 5.1.23.

W niektórych przypadkach bezpośrednio wykonanie pełnej aktualizacji (opisanej poniżej) może usunąć 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

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

W ten sposób zaktualizowane 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 proszony o 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

Proces aktualizacji do wydania bullseye może prosić o usunięcie pewnych pakietów. Dokładna lista będzie zależała od obecnie zainstalowanych pakietów. Niniejsze uwagi do wydania dają ogólny obraz tego zabiegu. W razie wątpliwości przed kontynuowaniem należy sprawdzić listę usuwanych pakietów proponowaną przez każdą z metod. Więcej informacji o pakietach przestarzałych w wydaniu bullseye znajduje się w Sekcja 4.8.

### 4.5.3 Konflikty lub pętle „wymaga wstępnie”

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

```
# 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 reguły 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 wyświetloną 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 konsolę, 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. Proszę zastąpić `F1` klawiszem funkcyjnym 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 terminale tekstowe.

## 4.6 Aktualizacja jądra 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.

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 5.1.25 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/) (<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.

- Usunięcie pakietów oznaczonych teraz jako przestarzałe zgodnie z opisem w rozdziałach Sekcja 4.4.3 i Sekcja 4.8. Proszę przejrzeć używane pliki konfiguracyjne i rozważyć całkowite wyczyszczenie (ang. `purge`) pakietów, w celu usunięcia ich plików konfiguracyjnych. Zob. też Sekcja 4.7.1.

### 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`.

**UWAGA!**

Wyczyszczenie pakietu zazwyczaj usuwa również jego pliki dziennika, dlatego można rozważyć uprzednie wykonanie ich kopii zapasowej.

Poniższe polecenie wyświetla listę wszystkich usuniętych pakietów z pozostawionymi w systemie plikami konfiguracyjnymi:

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

The packages can be removed by using **apt purge**. Assuming you want to purge all of them in one go, you can use the following command:

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

Jeśli korzysta się z programu **aptitude**, można rozważyć użycie następującego odpowiednika powyższych poleceń:

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

## 4.8 Przeszarzałe pakiety

Wprowadzając wiele nowych pakietów, bullseye porzuca i pomija również sporo 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<sup>5</sup> i nie dostarczy innego wsparcia 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 utrzymywany 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 **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:

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

**System śledzenia błędów Debiana** (<https://bugs.debian.org/>) często udostępnia dodatkowe informacje nt. powodów usunięcia danego pakietu. Należy przejrzeć zarówno archiwalne zgłoszenia błędów samego pakietu jak i archiwalne zgłoszenia **pseudopakietu ftp.debian.org** (<https://bugs.debian.org/cgi-bin/pkgreport.cgi?pkg=ftp.debian.org&archive=yes>).

Lista pakietów uznanych za przeszarzałe 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

<sup>5</sup>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

# Problemy, 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 New VA-API default driver for Intel GPUs

For Intel GPUs available with Broadwell and newer, the Video Acceleration API (VA-API) implementation now defaults to `intel-media-va-driver` for hardware accelerated video decoding. Systems which have `va-driver-all` installed will automatically be upgraded to the new driver.

The legacy driver package `i965-va-driver` is still available and offers support up to the Cannon Lake micro architecture. To prefer the legacy driver over the new default one, set the environment variable `LIBVA_DRIVER_NAME` to `i965`, for instance by setting the variable in `/etc/environment`. For more information, please see the Wiki's page on [hardware video acceleration](https://wiki.debian.org/HardwareVideoAcceleration) (<https://wiki.debian.org/HardwareVideoAcceleration>).

#### 5.1.2 The XFS file system no longer supports `barrier/nobarrier` option

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

#### 5.1.3 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 `/`).

### 5.1.4 Password hashing uses yescrypt by default

The default password hash for local system accounts **has been changed** (<https://tracker.debian.org/news/1226655/accepted-pam-140-3-source-into-unstable/>) from SHA-512 to **yescrypt** (<https://www.openwall.com/yescrypt/>) (see **crypt(5)** (<https://manpages.debian.org//bullseye/libcrypt-dev/crypt.5.html>)). 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`.

### 5.1.5 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.

### 5.1.6 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/>).

### 5.1.7 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.

### 5.1.8 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/>).

### 5.1.9 OpenStack and cgroups v1

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



### 5.1.10 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) (<https://governance.openstack.org/tc/goals/selected/wallaby/migrate-policy-format-from-json-to-yaml.html>).

### 5.1.11 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](#).

### 5.1.12 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.

### 5.1.13 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.

### 5.1.14 Linux enables user namespaces by default

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

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

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

```
user.max_user_namespaces = 0
```

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

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

### 5.1.15 Linux disables unprivileged calls to bpf() by default

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

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

```
kernel.unprivileged_bpf_disabled = 0
```

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

### 5.1.16 redmine missing in bullseye

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

### 5.1.17 Exim 4.94

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

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

Typical nonworking examples include:

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

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

instead of

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

for a virtual domain alias file.

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

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

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

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

### 5.1.18 SCSI device probing is non-deterministic

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

### 5.1.19 rdiff-backup require lockstep upgrade of server and client

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

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

### 5.1.20 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) (<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) (<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) (<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.

### 5.1.21 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) (<https://bugs.debian.org/988963>).

### 5.1.22 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/410a6ce5c80dd981c22752da034f2529b5eee8) (<https://github.com/fail2ban/fail2ban/commit/410a6ce5c80dd981c22752da034f2529b5eee8>) (which inserted the string `"-E 'set escape'"` in multiple places under `/etc/fail2ban/action.d/`).

### 5.1.23 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.

### 5.1.24 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) (<https://bugs.debian.org/989720>).

### 5.1.25 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<sup>1</sup> 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`,

<sup>1</sup>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`.

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.

### 5.2.3 The rescue boot option is unusable without a root password

With the implementation of `sudo` 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) (<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) (<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) (<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). (<https://docs.mailman3.org/en/latest/migration.html>)

- The Linux kernel no longer provides `isdn4linux (i4l)` support. Consequently, the related user-land packages `isdnutils`, `isdnactivecards`, `drdsl` and `ibod` have been removed from the archives.
- The deprecated `libappindicator` libraries are no longer provided. As a result, the related packages `libappindicator1`, `libappindicator3-1` and `libappindicator-dev` are no longer available. This is expected to cause dependency errors for third-party software that still depends on `libappindicator` to provide system tray and indicator support.

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

For background on the removal, see [the removal request](https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=963750) (<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.
- The `aufs-dkms` package is not part of bullseye. Most `aufs-dkms` users should be able to switch to `overlayfs`, which provides similar functionality with kernel support. However, it's possible to have a Debian installation on a filesystem that is not compatible with `overlayfs`, e.g. `xfs` without `d_type`. Users of `aufs-dkms` are advised to migrate away from `aufs-dkms` before upgrading to bullseye.
- The network connection manager `wicd` will no longer be available after the upgrade, so to avoid the danger of losing connectivity users are recommended to switch before the upgrade to an alternative such as `network-manager` or `connman`.

### 5.3.2 Przeszarżałe składniki w wydaniu bullseye

W następnym wydaniu 12 (nazwa kodowa: `bookworm`) niektóre funkcje zostaną porzucone. Proszę przejść na rozwiązania alternatywne, aby uniknąć problemów przy aktualizacji do Debian 12.

Obejmuje to poniższe funkcje:

- The historical justifications for the filesystem layout with `/bin`, `/sbin`, and `/lib` directories separate from their equivalents under `/usr` no longer apply today; see the [Freedesktop.org summary](https://www.freedesktop.org/wiki/Software/systemd/TheCaseForTheUsrMerge) (<https://www.freedesktop.org/wiki/Software/systemd/TheCaseForTheUsrMerge>). Debian bullseye will be the last Debian release that supports the non-merged-usr layout; for systems with a legacy layout that have been upgraded without a reinstall, the `usrmerge` package exists to do the conversion if desired.
- bullseye is the final Debian release to ship **apt-key**. Keys should be managed by dropping files into `/etc/apt/trusted.gpg.d` instead, in binary format as created by `gpg --export` with a `.gpg` extension, or ASCII armored with a `.asc` extension.

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

- The slapd database backends [slapd-bdb\(5\)](https://manpages.debian.org//bullseye/slapd/slapd-bdb.5.html) (<https://manpages.debian.org//bullseye/slapd/slapd-bdb.5.html>), [slapd-hdb\(5\)](https://manpages.debian.org//bullseye/slapd/slapd-hdb.5.html) (<https://manpages.debian.org//bullseye/slapd/slapd-hdb.5.html>), and [slapd-shell\(5\)](https://manpages.debian.org//bullseye/slapd/slapd-shell.5.html) (<https://manpages.debian.org//bullseye/slapd/slapd-shell.5.html>) are being retired and will not be included in Debian 12. LDAP databases using the `bdb` or `hdb` backends should be migrated to the [slapd-mdb\(5\)](https://manpages.debian.org//bullseye/slapd/slapd-mdb.5.html) (<https://manpages.debian.org//bullseye/slapd/slapd-mdb.5.html>) backend. Additionally, the [slapd-perl\(5\)](https://manpages.debian.org//bullseye/slapd/slapd-perl.5.html) (<https://manpages.debian.org//bullseye/slapd/slapd-perl.5.html>) and [slapd-sql\(5\)](https://manpages.debian.org//bullseye/slapd/slapd-sql.5.html) (<https://manpages.debian.org//bullseye/slapd/slapd-sql.5.html>) backends are deprecated and may be removed in a future release.

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

## 5.4 Known severe bugs

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

Bug number	Package (source or binary)	Description
<a href="https://bugs.debian.org/922981">922981</a> ( <a href="https://bugs.debian.org/922981">https://bugs.debian.org/922981</a> )	ca-certificates-java	ca-certificates-java: /etc/ca-certificates/update.d/jks-keystore doesn't update /etc/ssl/certs/java/cacerts
<a href="https://bugs.debian.org/990026">990026</a> ( <a href="https://bugs.debian.org/990026">https://bugs.debian.org/990026</a> )	cron	cron: Reduced charset in MAILTO causes breakage
<a href="https://bugs.debian.org/991081">991081</a> ( <a href="https://bugs.debian.org/991081">https://bugs.debian.org/991081</a> )	gir1.2-diodon-1.0	gir1.2-diodon-1.0 lacks dependencies
<a href="https://bugs.debian.org/990318">990318</a> ( <a href="https://bugs.debian.org/990318">https://bugs.debian.org/990318</a> )	python-pkg-resources	python-pkg-resources: please add Breaks against the unversioned python packages
<a href="https://bugs.debian.org/991449">991449</a> ( <a href="https://bugs.debian.org/991449">https://bugs.debian.org/991449</a> )	fail2ban	fix for CVE-2021-32749 breaks systems with mail from bsd-mailx
<a href="https://bugs.debian.org/990708">990708</a> ( <a href="https://bugs.debian.org/990708">https://bugs.debian.org/990708</a> )	mariadb-server-10.5, galera	mariadb-server-10.5: upgrade problems due to galera-3 -> galera-4 switch
<a href="https://bugs.debian.org/980429">980429</a> ( <a href="https://bugs.debian.org/980429">https://bugs.debian.org/980429</a> )	src:gcc-10	g++-10: spurious c++17 mode segmentation fault in append_to_statement_list_1 (tree-iterator.c:65)
<a href="https://bugs.debian.org/980609">980609</a> ( <a href="https://bugs.debian.org/980609">https://bugs.debian.org/980609</a> )	src:gcc-10	missing i386-cpuinfo.h
<a href="https://bugs.debian.org/984574">984574</a> ( <a href="https://bugs.debian.org/984574">https://bugs.debian.org/984574</a> )	gcc-10-base	gcc-10-base: please add Breaks: gcc-8-base (<< 8.4)
<a href="https://bugs.debian.org/984931">984931</a> ( <a href="https://bugs.debian.org/984931">https://bugs.debian.org/984931</a> )	git-el	git-el,elpa-magit: fails to install: /usr/lib/emacs-common/packages/install/git emacs failed at /usr/lib/emacs-common/lib.pl line 19, <TSORT> line 7.
<a href="https://bugs.debian.org/987264">987264</a> ( <a href="https://bugs.debian.org/987264">https://bugs.debian.org/987264</a> )	git-el	git-el: fails to install with xemacs21
<a href="https://bugs.debian.org/991082">991082</a> ( <a href="https://bugs.debian.org/991082">https://bugs.debian.org/991082</a> )	gir1.2-gtd-1.0	gir1.2-gtd-1.0 has empty Depends
<a href="https://bugs.debian.org/948739">948739</a> ( <a href="https://bugs.debian.org/948739">https://bugs.debian.org/948739</a> )	gparted	gparted should not mask .mount units
<a href="https://bugs.debian.org/984714">984714</a> ( <a href="https://bugs.debian.org/984714">https://bugs.debian.org/984714</a> )	gparted	gparted should suggest exfat-progs and backport the commit that rejects exfat-utils
<a href="https://bugs.debian.org/984760">984760</a> ( <a href="https://bugs.debian.org/984760">https://bugs.debian.org/984760</a> )	grub-efi-amd64	grub-efi-amd64: upgrade works, boot fails (error: symbol `grub_is_lockdown` not found)
<a href="https://bugs.debian.org/968368">968368</a> ( <a href="https://bugs.debian.org/968368">https://bugs.debian.org/968368</a> )	ifenslave	ifenslave: Option bond-master fails to add interface to bond
<a href="https://bugs.debian.org/990428">990428</a> ( <a href="https://bugs.debian.org/990428">https://bugs.debian.org/990428</a> )	ifenslave	ifenslave: Bonding not working on bullseye (using bond-slaves config)
<a href="https://bugs.debian.org/991113">991113</a> ( <a href="https://bugs.debian.org/991113">https://bugs.debian.org/991113</a> )	libpam-chroot	libpam-chroot installs pam_chroot.so into the wrong directory
<a href="https://bugs.debian.org/989545">989545</a> ( <a href="https://bugs.debian.org/989545">https://bugs.debian.org/989545</a> )	src:llvm-toolchain-11	libgl1-mesa-dri: si_texture.c:1727 si_texture_transfer_map - failed to create temporary texture to hold untiled copy

Bug number	Package (source or binary)	Description
<a href="https://bugs.debian.org/982459">982459</a> ( <a href="https://bugs.debian.org/982459">https://bugs.debian.org/982459</a> )	mdadm	mdadm --examine in chroot without /proc,/dev,/sys mounted corrupts host's filesystem
<a href="https://bugs.debian.org/981054">981054</a> ( <a href="https://bugs.debian.org/981054">https://bugs.debian.org/981054</a> )	openipmi	openipmi: Missing dependency on kmod
<a href="https://bugs.debian.org/948318">948318</a> ( <a href="https://bugs.debian.org/948318">https://bugs.debian.org/948318</a> )	openssh-server	openssh-server: Unable to restart sshd restart after upgrade to version 8.1p1-2
<a href="https://bugs.debian.org/991151">991151</a> ( <a href="https://bugs.debian.org/991151">https://bugs.debian.org/991151</a> )	procps	procps: dropped the reload option from the init script, breaking corekeeper
<a href="https://bugs.debian.org/989103">989103</a> ( <a href="https://bugs.debian.org/989103">https://bugs.debian.org/989103</a> )	pulseaudio	pulseaudio regressed on control = Wave configuration
<a href="https://bugs.debian.org/984580">984580</a> ( <a href="https://bugs.debian.org/984580">https://bugs.debian.org/984580</a> )	libpython3.9-dev	libpython3.9-dev: missing dependency on zlib1g-dev
<a href="https://bugs.debian.org/990417">990417</a> ( <a href="https://bugs.debian.org/990417">https://bugs.debian.org/990417</a> )	src:qemu	openjdk-11-jre-headless: running java in qemu s390 gives a SIGILL at C [linux-vdso64.so.1 + 0x6f8] _kernel_getcpu + 0x8
<a href="https://bugs.debian.org/859926">859926</a> ( <a href="https://bugs.debian.org/859926">https://bugs.debian.org/859926</a> )	speech-dispatcher	breaks with pulse-audio as output when spawned by speechd-up from init system
<a href="https://bugs.debian.org/932501">932501</a> ( <a href="https://bugs.debian.org/932501">https://bugs.debian.org/932501</a> )	src:squid-deb-proxy	squid-deb-proxy: daemon does not start due to the conf file not being allowed by apparmor
<a href="https://bugs.debian.org/991588">991588</a> ( <a href="https://bugs.debian.org/991588">https://bugs.debian.org/991588</a> )	tpm2-abrmd	tpm2-abrmd should not use Requires = systemd-udev-settle.service in its unit
<a href="https://bugs.debian.org/991939">991939</a> ( <a href="https://bugs.debian.org/991939">https://bugs.debian.org/991939</a> )	libjs-bootstrap4	libjs-bootstrap4: broken symlinks: /usr/share/javascript/bootstrap4/css/bootstrap*.css.map -> ../../../../nodejs/bootstrap/dist/css/bootstrap*.css.map
<a href="https://bugs.debian.org/991822">991822</a> ( <a href="https://bugs.debian.org/991822">https://bugs.debian.org/991822</a> )	src:wine	src:wine: dh_auto_clean deletes unrelated files outside of package source
<a href="https://bugs.debian.org/988477">988477</a> ( <a href="https://bugs.debian.org/988477">https://bugs.debian.org/988477</a> )	src:xen	xen-hypervisor-4.14-amd64: xen dmesg shows (XEN) AMD-Vi: IO_PAGE_FAULT on sata pci device
<a href="https://bugs.debian.org/991788">991788</a> ( <a href="https://bugs.debian.org/991788">https://bugs.debian.org/991788</a> )	xfce4-settings	xfce4-settings: black screen after suspend when laptop lid is closed and re-opened



## Rozdział 6

# Więcej informacji na temat projektu Debian

### 6.1 Dodatkowe informacje

Poza uwagami do wydania i przewodnikiem po instalacji dostępna jest również dodatkowa dokumentacja na temat systemu Debian, pochodząca z Projektu Dokumentacji Debiana (DDP), którego zadaniem jest tworzenie wysokiej jakości dokumentacji dla użytkowników i deweloperów Debiana. Dostępne są dokumenty Debian Reference, Debian New Maintainers' Guide i FAQ Debiana oraz wiele innych. Pełny spis wszystkich zasobów można znaleźć na [stronie z dokumentacją Debiana](https://www.debian.org/doc/) (<https://www.debian.org/doc/>) (proszę zwrócić uwagę na odnośnik do polskiej dokumentacji w dolnej części strony) i w [Wiki Debiana](https://wiki.debian.org/) (<https://wiki.debian.org/>).

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

Najbardziej interesującymi dla użytkowników Debiana listami dyskusyjnymi są: `debian-user` (angielska) i listy dla poszczególnych języków: `debian-user-język` (np. `debian-user-polish` - polska lista). Więcej informacji i szczegóły na temat subskrypcji zawiera strona <https://lists.debian.org/>. Przed zamieszczeniem nowej wiadomości prosimy o uprzednie przeszukanie archiwów listy, które może już zawierać odpowiedź na zadawane pytanie; proszę również pamiętać o zachowaniu netykiety.

#### 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.

Proszę przestrzegać zasad kanału respektując prawa innych użytkowników. Wytyczne są dostępne na [Wiki Debiana](https://wiki.debian.org/DebianIRC) (<https://wiki.debian.org/DebianIRC>).

Więcej informacji o OFTC można znaleźć na odpowiedniej [stronie internetowej](http://www.oftc.net/) (<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 spakietowanym 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.

Jeśli ma się nieco więcej czasu można poświęcić go jakiejś części Wolnego Oprogramowania w Debianie. Szczególnie pożądane jest, aby adoptować lub zacząć opiekować się pakietami, o których dodanie prosili inni użytkownicy. Baza **Work Needing and Prospective Packages** (<https://www.debian.org/devel/wnpp/>) dostarcza szczegółowych informacji w tym zakresie. Jeśli jest się szczególnie zainteresowanym jakąś konkretną dziedziną to można włożyć swój wkład w któryś z **podprojektów** (<https://www.debian.org/devel/#projects>) Debiana, które zajmują się również portami na różne architektury lub w tzw. **Debian Pure Blends** (<https://wiki.debian.org/DebianPureBlends>), przeznaczonych dla określonych grup użytkowników, albo w wiele innych.

W każdym razie, niezależnie 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 szeregową)

**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

```
# apt update
```

aby odświeżyć listę pakietów.

### A.3 Usunięcie przestarzałych plików konfiguracyjnych

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

## Dodatek B

# Współtwórcy uwag do wydania

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

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

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

Polskie tłumaczenie: Michał Kułach i Wojciech Zaręba. Cenne wskazówki i uwagi wnieśli: Bolesław Śliwicki i Paweł Sadkowski.





# 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

ca-certificates-java, 33

chef, 31

cinder-volume, 26

connman, 32

cron, 33

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

grub-efi-amd64, 33

grub2, 31

guile-2.2-libs, 29

gvfs-fuse, 27

how-can-i-help, 36

i965-va-driver, 25

ibod, 31

ifenslave, 33

initramfs-tools, 10, 21

intel-media-va-driver, 25

intel-microcode, 29

ipp-usb, 4, 5

isdnactivecards, 31

isdnutils, 31

kio-fuse, 27

libappindicator-dev, 31

libappindicator1, 31

libappindicator3-1, 31

libayatana-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, 34  
network-manager, 32  
nova-compute, 26  
openipmi, 34  
openssh-server, 29, 34  
openvswitch, 29  
popularity-contest, 17  
procps, 34  
pulseaudio, 34  
python-pkg-resources, 33  
python-setuptools, 32  
rails, 28  
rdiff-backup, 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  
va-driver-all, 25  
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