

Информация о выпуске Debian 11 (bullseye) для архитектуры 64-bit PC

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

26 июня 2022 г.

Информация о выпуске Debian 11 (bullseye) для архитектуры 64-bit PC

This document is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License, version 2, as published by the Free Software Foundation.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 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.

Оглавление

| | | |
|----------|--|-----------|
| 1 | Введение | 1 |
| 1.1 | Как сообщить об ошибке в этом документе | 1 |
| 1.2 | Предоставление отчёта об обновлении | 1 |
| 1.3 | Исходный текст этого документа | 2 |
| 2 | Что нового в Debian 11 | 3 |
| 2.1 | Поддерживаемые архитектуры | 3 |
| 2.2 | Что нового в дистрибутиве? | 3 |
| 2.2.1 | Desktops and well known packages | 3 |
| 2.2.2 | Driverless scanning and printing | 5 |
| 2.2.2.1 | CUPS and driverless printing | 5 |
| 2.2.2.2 | SANE and driverless scanning | 5 |
| 2.2.3 | New generic open command | 6 |
| 2.2.4 | Control groups v2 | 6 |
| 2.2.5 | Persistent systemd journal | 6 |
| 2.2.6 | New Fcitx 5 Input Method | 6 |
| 2.2.7 | Новости Debian Med | 6 |
| 2.2.8 | Kernel support for exFAT | 6 |
| 2.2.9 | Improved man page translations | 7 |
| 2.2.10 | Improved support for alternative init systems | 7 |
| 3 | Система установки | 9 |
| 3.1 | Что нового в системе установки? | 9 |
| 3.1.1 | Help with installation of firmware | 9 |
| 3.1.2 | Автоматизированная установка | 9 |
| 3.2 | Cloud installations | 10 |
| 3.3 | Container and Virtual Machine images | 10 |
| 4 | Обновление с Debian 10 (buster) | 11 |
| 4.1 | Подготовка к обновлению | 11 |
| 4.1.1 | Создание резервной копии всех данных и настроек | 11 |
| 4.1.2 | Предварительное информирование пользователей | 11 |
| 4.1.3 | Подготовка к перерыву в работе служб | 11 |
| 4.1.4 | Подготовка к восстановлению | 12 |
| 4.1.4.1 | Отладочная оболочка из initrd во время загрузки | 12 |
| 4.1.4.2 | Отладочная оболочка во время загрузки с использованием systemd | 12 |
| 4.1.5 | Подготовка безопасного окружения для обновления | 13 |
| 4.2 | Start from «pure» Debian | 13 |
| 4.2.1 | Upgrade to Debian 10 (buster) | 13 |
| 4.2.2 | Remove non-Debian packages | 13 |
| 4.2.3 | Upgrade to latest point release | 14 |
| 4.2.4 | Prepare the package database | 14 |
| 4.2.5 | Remove obsolete packages | 14 |
| 4.2.6 | Clean up leftover configuration files | 14 |
| 4.2.7 | The security section | 14 |
| 4.2.8 | Секция proposed-updates | 14 |
| 4.2.9 | Неофициальные источники | 14 |
| 4.2.10 | Отключение фиксации в APT | 14 |
| 4.2.11 | Check package status | 15 |
| 4.3 | Preparing APT source-list files | 15 |
| 4.3.1 | Добавление интернет-источников в APT | 16 |
| 4.3.2 | Добавление локального зеркала в качестве источника APT | 16 |
| 4.3.3 | Добавление оптического носителя в качестве источника APT | 17 |
| 4.4 | Обновление пакетов | 17 |

| | | |
|----------|--|-----------|
| 4.4.1 | Запись сеанса | 18 |
| 4.4.2 | Обновление списка пакетов | 18 |
| 4.4.3 | Проверка доступного пространства для обновления | 18 |
| 4.4.4 | Минимальное обновление системы | 20 |
| 4.4.5 | Обновление системы | 21 |
| 4.5 | Возможные проблемы во время обновления | 21 |
| 4.5.1 | Dist-upgrade завершается с ошибкой «Could not perform immediate configuration» | 21 |
| 4.5.2 | Ожидаемые удаления | 21 |
| 4.5.3 | Конфликты или заикливание в требованиях предварительной установки | 22 |
| 4.5.4 | Файловые конфликты | 22 |
| 4.5.5 | Изменение настроек | 22 |
| 4.5.6 | Изменение консоли сеанса | 23 |
| 4.6 | Обновление ядра и сопутствующих пакетов | 23 |
| 4.6.1 | Установка метапакета ядра | 23 |
| 4.7 | Подготовка к следующему выпуску | 24 |
| 4.7.1 | Вычистка удалённых пакетов | 24 |
| 4.8 | Устаревшие пакеты | 24 |
| 4.8.1 | Transitional dummy packages | 25 |
| 5 | Что нужно знать о bullseye | 27 |
| 5.1 | Конкретные шаги обновления для bullseye | 27 |
| 5.1.1 | New VA-API default driver for Intel GPUs | 27 |
| 5.1.2 | The XFS file system no longer supports barrier/nobarrier option | 27 |
| 5.1.3 | Changed security archive layout | 27 |
| 5.1.4 | Password hashing uses yescrypt by default | 28 |
| 5.1.5 | NSS NIS and NIS+ support require new packages | 28 |
| 5.1.6 | Config file fragment handling in unbound | 28 |
| 5.1.7 | rsync parameter deprecation | 28 |
| 5.1.8 | Vim addons handling | 28 |
| 5.1.9 | OpenStack and cgroups v1 | 28 |
| 5.1.10 | OpenStack API policy files | 29 |
| 5.1.11 | sendmail downtime during upgrade | 29 |
| 5.1.12 | FUSE 3 | 29 |
| 5.1.13 | GnuPG options file | 29 |
| 5.1.14 | Linux enables user namespaces by default | 29 |
| 5.1.15 | Linux disables unprivileged calls to bpf() by default | 29 |
| 5.1.16 | redmine missing in bullseye | 30 |
| 5.1.17 | Exim 4.94 | 30 |
| 5.1.18 | SCSI device probing is non-deterministic | 30 |
| 5.1.19 | rdiff-backup require lockstep upgrade of server and client | 31 |
| 5.1.20 | Intel CPU microcode issues | 31 |
| 5.1.21 | Upgrades involving libgc1c2 need two runs | 31 |
| 5.1.22 | fail2ban can't send e-mail using mail from bsd-mailx | 31 |
| 5.1.23 | No new SSH connections possible during upgrade | 31 |
| 5.1.24 | Open vSwitch upgrade requires interfaces(5) change | 31 |
| 5.1.25 | То, что следует сделать после обновления и до перезагрузки | 32 |
| 5.2 | Items not limited to the upgrade process | 32 |
| 5.2.1 | Ограничения поддержки безопасности | 32 |
| 5.2.1.1 | Security status of web browsers and their rendering engines | 32 |
| 5.2.1.2 | OpenJDK 17 | 32 |
| 5.2.1.3 | Go-based packages | 32 |
| 5.2.2 | Accessing GNOME Settings app without mouse | 32 |
| 5.2.3 | The rescue boot option is unusable without a root password | 33 |
| 5.3 | Obsolescence and deprecation | 33 |
| 5.3.1 | Заслуживающие внимания устаревшие пакеты | 33 |
| 5.3.2 | Устаревшие компоненты bullseye | 34 |
| 5.4 | Known severe bugs | 34 |

| | | |
|----------|--|-----------|
| 6 | Дополнительная информация о Debian | 37 |
| 6.1 | Что ещё можно прочитать | 37 |
| 6.2 | Если нужна помощь | 37 |
| 6.2.1 | Списки рассылки | 37 |
| 6.2.2 | IRC | 37 |
| 6.3 | Как сообщить об ошибке | 38 |
| 6.4 | Как помочь Debian | 38 |
| 7 | Глоссарий | 39 |
| A | Подготовка системы buster к обновлению | 41 |
| A.1 | Обновление системы buster | 41 |
| A.2 | Checking your APT source-list files | 41 |
| A.3 | Удаление устаревших файлов настройки | 42 |
| B | Люди, участвовавшие в создании информации о выпуске | 43 |
| | Предметный указатель | 45 |

Глава 1

Введение

Данный документ информирует пользователей дистрибутива Debian об основных изменениях в выпуске 11 (bullseye).

В информации о выпуске описывается процесс безопасного обновления с выпуска 10 (buster) до текущего выпуска и известные потенциальные проблемы, с которыми могут столкнуться пользователи при обновлении.

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

ПРЕДОСТЕРЕЖЕНИЕ



Заметим, что здесь невозможно перечислить все известные проблемы, и поэтому были выбраны только те, которые, как ожидается, могут возникнуть у большинства людей, и которые оказывают наибольшее влияние в целом.

Обратите внимание, что теперь поддерживается и описывается только обновление с предыдущего выпуска Debian (то есть, этот документ описывает обновление с buster). Если вам требуется обновить систему с более старого выпуска, обратитесь к ранним редакциям этого документа или сначала выполните обновление до buster.

1.1 Как сообщить об ошибке в этом документе

Мы пытались провести все возможные этапы обновления, описанные в этом документе, а также попытались предвидеть все возможные проблемы, с которыми могут столкнуться пользователи.

Тем не менее, если вы думаете, что нашли ошибку в этом описании (есть неправильная или отсутствующая информация), пожалуйста, отправьте сообщение об ошибке в пакете `release-notes` в [систему отслеживания ошибок](https://bugs.debian.org/) (<https://bugs.debian.org/>). Не забудьте сначала просмотреть [существующие сообщения об ошибках](https://bugs.debian.org/release-notes) (<https://bugs.debian.org/release-notes>), возможно, о вашей проблеме уже известно. В этом случае вы можете послать дополнительную информацию к существующему сообщению об ошибке или даже предложить свои изменения.

Мы были бы очень благодарны, если к сообщению была бы приложена заплата, исправляющая исходный текст документа. О том, где взять исходный текст данного документа, см. Раздел [1.3](#).

1.2 Предоставление отчёта об обновлении

Мы рады любой информации о проведённом обновлении с buster до bullseye от пользователей. Если вы хотите поделиться своим опытом, отправьте сообщение об ошибке в пакете `upgrade-reports` в [систему отслеживания ошибок](https://bugs.debian.org/) (<https://bugs.debian.org/>), описав результаты. Пожалуйста, сжимайте все прилагаемые к сообщению файлы (с помощью `gzip`).

Пожалуйста, включите в отправляемое сообщение следующую информацию:

- Состояние вашей базы данных пакетов до и после обновления: состояние базы данных `dpkg` содержится в файле `/var/lib/dpkg/status`, а информация о состоянии пакетов `apt` — в файле `/var/lib/apt/extended_states`. Перед обновлением выполните резервное копирование согласно описанию Раздел 4.1.1, помимо этого, вы можете найти резервные копии `/var/lib/dpkg/status` в каталоге `/var/backups`.
- Журналы сеанса работы, созданные с помощью `script`, см. Раздел 4.4.1.
- Журнал работы `apt` доступен в файле `/var/log/apt/term.log` или журнал `aptitude` доступен в каталоге `/var/log/aptitude`.

ЗАМЕЧАНИЕ



Обязательно просмотрите и удалите всю личную и/или конфиденциальную информацию из журналов перед тем как включать их в сообщение об ошибке, так как эта информация будет занесена в доступную всем базу данных.

1.3 Исходный текст этого документа

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>).

Глава 2

Что нового в Debian 11

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

2.1 Поддерживаемые архитектуры

Список официально поддерживаемых архитектур для Debian 11:

- 32-битный ПК (i386) и 64-битный ПК (amd64)
- 64-битный ARM (arm64)
- ARM EABI (armel)
- ARMv7 (EABI hard-float ABI, armhf)
- little-endian MIPS (mipsel)
- 64-битный MIPS с порядком байтов от младшего к старшему (mips64el)
- 64-битный PowerPC с порядком байтов от младшего к старшему (ppc64el)
- IBM System z (s390x)

Более подробную информацию о переносе на различные архитектуры и сведения, относящиеся к конкретным переносам, вы можете получить на [странице переносов Debian](https://www.debian.org/ports/) (<https://www.debian.org/ports/>).

2.2 Что нового в дистрибутиве?

Новый выпуск Debian опять содержит намного больше программ, чем его предшественник, buster. Дистрибутив включает в себя более 11294 новых пакетов, всего их стало более 59551. Большая часть программ, входящих в дистрибутив, была обновлена: более 42821 пакетов (что составляет 72% дистрибутива buster). Также, по различным причинам многие пакеты (более 9519, 16% дистрибутива buster) были удалены из дистрибутива. Эти пакеты не будут обновляться, в инструментах управления пакетами они будут помечены как "устаревшие" (obsolete), см. Раздел [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.

Также были обновлены офисные приложения, включая следующие комплекты:

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

- GNUcash is upgraded to 4.4;

В этом выпуске, среди прочего, было обновлено следующее программное обеспечение:

| Пакет | Версия в 10 (buster) | Версия в 11 (bullseye) |
|--|---------------------------|----------------------------|
| Apache | 2.4.38 | 2.4.48 |
| BIND DNS сервер | 9.11 | 9.16 |
| Cryptsetup | 2.1 | 2.3 |
| Dovecot MTA | 2.3.4 | 2.3.13 |
| Emacs | 26.1 | 27.1 |
| Exim, почтовый сервер по умолчанию | 4.92 | 4.94 |
| GNU Compiler Collection, компилятор по умолчанию | 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 |
| GNU библиотека C | 2.28 | 2.31 |
| lighttpd | 1.4.53 | 1.4.59 |
| Образ ядра 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 Раздел 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 add-on support. More information including the migration guide can be found on the wiki (<https://wiki.debian.org/I18n/Fcix5>).

2.2.7 Новости 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) (<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>).

Глава 3

Система установки

Debian Installer (программа установки) является официальной системой установки Debian. Она предлагает широкий выбор методов установки. Список доступных методов зависит от архитектуры компьютера.

Образы программы установки для bullseye и руководство по установке можно найти на [веб-сайте Debian](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/ru/index.html
```

Также следует ознакомиться со списком [известных ошибок](https://www.debian.org/releases/bullseye/debian-installer/index#errata) (<https://www.debian.org/releases/bullseye/debian-installer/index#errata>) программы установки.

3.1 Что нового в системе установки?

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)). 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 Автоматизированная установка

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.

В [руководстве по установке](https://www.debian.org/releases/bullseye/installmanual) (<https://www.debian.org/releases/bullseye/installmanual>) теперь есть отдельное приложение, в котором подробно описывается использование автоматизированной настройки.

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>).

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

Глава 4

Обновление с Debian 10 (buster)

4.1 Подготовка к обновлению

Перед обновлением мы рекомендуем вам также прочитать Глава 5. Этот раздел описывает потенциальные проблемы, которые не имеют прямого отношения к процессу обновления, но всё же важно узнать о них до установки.

4.1.1 Создание резервной копии всех данных и настроек

Перед обновлением настоятельно рекомендуется сделать резервную копию всей системы или, по крайней мере, всех данных и настроек, которые вы не можете позволить себе потерять. Инструменты для обновления и сам процесс достаточно надёжны, но сбой аппаратного обеспечения в ходе обновления может привести к серьёзному повреждению системы.

В первую очередь необходимо сделать резервную копию содержимого каталогов `/etc`, `/var/lib/dpkg`, `/var/lib/apt/extended_states` и результата работы команды `dpkg --get-selections "*" (кавычки важны)`. Если для управления пакетами вы используете **aptitude**, то также сделайте резервную копию `/var/lib/aptitude/pkgstates`.

Обновление само по себе никак не затрагивает каталог `/home`. Однако некоторые приложения (в частности, некоторые приложения Mozilla, окружения рабочего стола GNOME и KDE) при первом запуске новой версии перезаписывают имеющиеся пользовательские настройки новыми настройками по умолчанию. На всякий случай стоит сделать резервную копию скрытых файлов и каталогов (название которых начинается с точки) из домашних каталогов пользователей. Это поможет вам в случае необходимости восстановить старые настройки. Не лишним будет предупредить пользователей об этой проблеме.

Установка любого пакета должна производиться с привилегиями суперпользователя. Поэтому вы должны либо войти в систему под именем суперпользователя `root`, либо использовать программы `su` или `sudo`, чтобы получить необходимые права.

Для проведения обновления есть несколько предварительных требований; проверьте, что они соблюдаются.

4.1.2 Предварительное информирование пользователей

Желательно заранее сообщать всем пользователям о любых планируемых обновлениях, хотя пользователи, работающие в системе через `ssh`, не должны испытать особых проблем в процессе обновления и вполне могут продолжать работу.

Если вы хотите принять дополнительные меры предосторожности, создайте резервную копию и размонтируйте раздел `/home` перед обновлением.

При обновлении до `bullseye` потребуется обновить ядро, поэтому потребуется перезагрузка. Обычно, это происходит по окончании обновления.

4.1.3 Подготовка к перерыву в работе служб

При обновлении может потребоваться обновить пакеты для работающих на данной машине служб. В этом случае работа служб будет прервана на время обновления, замены и настройки пакетов.

Точное время простоя служб будет зависеть от количества обновляемых в системе пакетов, а также от времени, затрачиваемое администратором для ответов на вопросы о настройке. Заметим, что если процесс обновления оставить без внимания и не следить за запросами системы, то высока вероятность увеличить недоступность служб¹ на значительный промежуток времени.

Если обновляемая система предоставляет критически важные службы для пользователей или сети², то вы можете сократить время простоя, если сначала выполните минимальное обновление системы (см. Раздел 4.4.4), затем обновите ядро и перезагрузитесь, а затем обновите пакеты, связанные с вашими критическими службами. Описание обновления этих пакетов перед полным обновлением смотрите в Раздел 4.4.5. Такой порядок позволяет оставить работающими критические службы на время прохождения полного обновления и сократить время простоя.

4.1.4 Подготовка к восстановлению

Хотя Debian пытается проверить, что система всегда будет в состоянии загрузиться, есть реальная опасность возникновения проблем после перезагрузки в обновлённую систему. Большая часть возможных проблем описана здесь и далее в следующих главах информации о выпуске.

Поэтому лучше удостовериться, что вы сможете вернуть систему в прежнее состояние, если она не сможет загрузиться или, для систем управляемых удалённо, не заработает сеть.

Если обновление производится удалённо через **ssh**, рекомендуем вам предусмотреть подключение к локальной консоли сервера через удалённый последовательный терминал. Может случиться так, что после обновления ядра и перезагрузки, вам потребуется исправить системные настройки через локальную консоль. Если система случайно перезагрузится в середине процесса обновления, вам также потребуется локальная консоль для восстановления.

Для аварийного восстановления обычно мы рекомендуем использовать *режим восстановления* из программы установки Debian bullseye. Преимущество в использовании программы установки состоит в том, что вы можете выбирать из множества методов установки тот, который лучше подходит в вашей ситуации. Дополнительная информация приведена в разделе «Восстановление сломанной системы» главы 8 *руководства по установке* (<https://www.debian.org/releases/bullseye/installmanual>) и в *ЧаВО по программе установки Debian* (<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 Отладочная оболочка из **initrd** во время загрузки

Пакет **initramfs-tools** добавляет отладочную оболочку³ в создаваемый **initrd**. Например, если **initrd** не удастся смонтировать корневую файловую систему, то вы попадёте в эту отладочную оболочку; она предоставляет основные команды, которые помогут вам выяснить в чём дело и, возможно, даже всё исправить.

Что нужно проверить: наличие правильных файлов устройств в каталоге `/dev`; какие модули загружены (`cat /proc/modules`); проверить в результатах **dmesg** отсутствие ошибок при загрузке драйверов. Вывод **dmesg** также покажет соответствие назначенных файлов устройств дискам; убедитесь, что результатом `echo $ROOT` является ожидаемое устройство для корневой файловой системы.

Если вы решили проблему, для выхода из отладочной оболочки наберите `exit`, и процесс загрузки продолжится с места останова. Естественно, вам нужно устранить причину и пересоздать **initrd** для того, чтобы следующая загрузка прошла без проблем.

4.1.4.2 Отладочная оболочка во время загрузки с использованием **systemd**

Если не удаётся загрузиться под **systemd**, можно запустить командную оболочку с правами суперпользователя, изменив строку команд ядра. Если базовая загрузка завершается успешно, но неко-

¹Если приоритет `debconf` установлен в самый высокий уровень, то ответов на вопросы о настройке можно избежать, но возможна ситуация, при которой ответы по умолчанию могут оказаться некорректны в вашей системе и службы могут не запуститься.

²Например: службы DNS или DHCP, а именно, когда не предусмотрены резервные серверы. В отсутствии DHCP пользователи могут быть отключены от сети, если время аренды меньше чем время, затрачиваемое на обновление.

³Эту возможность можно выключить, добавив параметр `panic=0` в параметры загрузки.

торые службы не запускаются, может быть полезным добавить команду `systemd.unit=rescue.target` к параметрам ядра.

В противном случае параметр ядра `systemd.unit=emergency.target` как можно раньше предоставит вам командную оболочку с правами суперпользователя. Тем не менее, это выполняется до монтирования корневой файловой системы с правами на чтение. Вам придётся выполнить это вручную с помощью следующей команды:

```
# 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 Подготовка безопасного окружения для обновления

ВАЖНО



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

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

4.2 Start from «pure» Debian

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

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

4.2.1 Upgrade to Debian 10 (buster)

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

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

Please follow the instructions in the [Release Notes for Debian 10](https://www.debian.org/releases/buster/releasenotes) (<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 Раздел [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 Раздел [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 Раздел [5.1.3](#).

4.2.8 Секция 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 Неофициальные источники

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.

У некоторых пользователей могут быть установлены *неофициальные* перенесённые «более новые» версии пакетов, собранные для *buster*. Такие пакеты, скорее всего, станут причиной проблем при обновлении, так как они могут вызвать конфликты файлов⁴. В Раздел [4.5](#) содержится некоторая информация о том, что делать, если возникли файловые конфликты.

4.2.10 Отключение фиксации в APT

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

⁴Обычно, система управления пакетами Debian не позволяет пакету удалить или заменить файл, принадлежащий другому пакету, за исключением случаев, когда явно указано, что один пакет заменяет другой.

4.2.11 Check package status

Независимо от способа обновления, рекомендуется сначала проверить состояние всех пакетов и убедиться, что всем пакетам разрешено обновляться. Следующая команда покажет пакеты установленные частично (Half-Installed), настройка которых не удалась (Failed-Config), а также все пакеты в ошибочных состояниях:

```
# dpkg --audit
```

Можно также проверить состояние всех пакетов системы с помощью программы **aptitude** и таких команд, как

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

или

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

Перед обновлением желательно снять все фиксации с пакетов. Если один из значимых для обновления пакетов зафиксирован, обновление завершится неудачно.

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$'
```

Если вы изменяли и перекомпилировали какой-то из пакетов локально, но при этом не переименовали его и не добавили «эпоху» к версии пакета, то его нужно зафиксировать, чтобы предотвратить обновление.

The «hold» package state for **apt** can be changed using:

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

Замените `hold` на `install`, чтобы отменить фиксацию.

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 Раздел [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.

На выпуск Debian часто ссылаются по его кодовому имени (например, `buster`, `bullseye`) или по его статусу (например, `oldstable` (старый стабильный), `stable` (стабильный), `testing` (тестируемый), `unstable` (нестабильный)). Ссылки на выпуск по кодовому имени имеют то преимущество, что вы никогда неожиданно для себя не начнёте пользоваться новым выпуском. Поэтому мы здесь так и делаем. В этом случае вам, конечно, придётся самим следить за анонсами новых выпусков. Если вы будете ссылаться на дистрибутив по его статусному имени, то после выхода нового выпуска вы просто увидите большое количество обновлённых пакетов.

Debian предоставляет два информационных списка рассылки, которые помогут вам оставаться в курсе событий и получать важную информацию о выпусках Debian:

- Подписавшись на **информационный список рассылки Debian** (<https://lists.debian.org/debian-announce/>), вы будете получать уведомления каждый раз, как Проект Debian создаёт новый выпуск. Например, когда bullseye становится из testing, к примеру, stable.
- Подписавшись на **информационный список рассылки Debian по вопросам безопасности** (<https://lists.debian.org/debian-security-announce/>), вы будете получать уведомления каждый раз, когда Проект Debian публикует информационное сообщение о безопасности.

4.3.1 Добавление интернет-источников в APT

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).

Например, допустим наиболее близким зеркалом Debian является <http://mirrors.kernel.org>. Если вы обратитесь к этому зеркалу с помощью веб-браузера, то вы заметите, что основные каталоги организованы следующим образом:

```
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
```

Заметим, что «dists» добавляется автоматически, а параметры после имени выпуска используются для дополнения сетевого пути до реальных каталогов.

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

4.3.2 Добавление локального зеркала в качестве источника APT

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).

Например, если ваше зеркало пакетов находится в каталоге `/var/local/debian/`, то его основные каталоги будут называться:

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

Чтобы пакет `apt` мог использовать этот источник пакетов, добавьте в файл `sources.list`:

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

Заметим, что «dists» добавляется автоматически, а параметры после имени выпуска используются для дополнения сетевого пути до реальных каталогов.

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 Добавление оптического носителя в качестве источника APT

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.

Убедитесь в том, что в файле `/etc/fstab` есть строка, позволяющая смонтировать компакт-диск в каталог `/media/cdrom`. Например, если файлом устройства вашего привода чтения компакт-дисков служит `/dev/sr0`, то файл `/etc/fstab` должен содержать строку:

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

Обратите внимание на то, что между словами `noauto,ro` в четвёртом поле строки *не должно быть пробелов*.

Чтобы проверить, что строка `fstab` написана верно, вставьте компакт-диск в привод и выполните команды

```
# 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
```

Затем выполните команду

```
# apt-cdrom add
```

для каждого компакт-диска Debian Binary, чтобы добавить все диски в базу данных APT.

4.4 Обновление пакетов

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

ЗАМЕЧАНИЕ



`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.

Не забудьте смонтировать все необходимые разделы (в первую очередь, корневой раздел и каталог `/usr`) на чтение и запись. Это можно сделать командой

```
# 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.

ЗАМЕЧАНИЕ



Строки источников для CD-ROM часто ссылаются на «unstable», хотя это может показаться странным, но исправлять их *не нужно*.

4.4.1 Запись сеанса

Для записи ваших действий при обновлении настоятельно рекомендуем использовать программу `/usr/bin/script`. В этом случае, при возникновении каких-либо проблем у вас будет журнал произошедших событий, и если понадобится, вы сможете включить эту информацию в отчёт об ошибке. Чтобы начать запись, выполните команду:

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

или похожую. При перезапуске записи (например, при перезагрузке системы) используйте другое значение вместо `step`, чтобы различать протоколируемые шаги. Не размещайте файл с записью во временных каталогах, таких как `/tmp` и `/var/tmp` (файлы в этих каталогах могут быть удалены при обновлении или перезагрузке).

Запись также поможет вам прочитать информацию, которая вышла за пределы экрана. Если вы находитесь перед монитором компьютера просто переключитесь на вторую консоль VT2 (нажав `Alt+F2`) и, войдя в систему, запустите `less -R ~/root/upgrade-bullseye.script` для просмотра файла.

После завершения обновления можно остановить `script`, набрав `exit` в командной строке.

`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`.

Если параметром к `script` указать `-t`, то вы сможете воспользоваться программой `scriptreplay` для повтора всего сеанса:

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

4.4.2 Обновление списка пакетов

Во-первых, нужно обновить список доступных пакетов нового выпуска. Это делается командой:

```
# apt update
```

ЗАМЕЧАНИЕ



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 Проверка доступного пространства для обновления

Перед обновлением всей системы, как описано в Раздел 4.4.5, убедитесь, что у вас достаточно места на диске. Сначала все нужные для установки пакеты скачиваются из сети и сохраняются в `/var/cache/apt/archives` (а на время скачивания, в подкаталог `partial/`), поэтому вы должны проверить место на разделе, который содержит `/var/`, так как туда будут временно записаны загруженные пакеты для установки. После загрузки вам, вероятно, понадобится дополнительное место в других разделах файловой системы для установки обновляемых пакетов (скорее всего, они стали больше) и новых пакетов, которые будут установлены из-за обновлений. Если в системе не будет достаточно места, то в конечном счёте это приведёт к неполному обновлению, что позднее бывает сложно исправить.

`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.
```

ЗАМЕЧАНИЕ



Запуск этой команды в начале процесса обновления может приводить к ошибке по причинам, описанным далее. В этом случае, запуск команды оценки дискового пространства нужно провести после выполнения минимального обновления системы (см. Раздел 4.4.4) и обновления ядра.

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/.
```

В этом случае освободите место заранее. Вы можете:

- 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
```

Существуют и другие инструменты для определения неиспользуемых пакетов, например, **deborphan**, **debfoaster** и **cruft**. Не удаляйте подряд все пакеты, найденные такими инструментами (в особенности, если при запуске вы указали параметры, отличные от умолчательных), чтобы не удалить что-нибудь нужное. Настоятельно рекомендуем перед удалением внимательно просмотреть список предложенных пакетов (прочитать описание, посмотреть входящие файлы и размер).

- Удалить пакеты, которые занимают слишком много места и в данный момент не нужны (вы всегда можете установить их снова после обновления). Если установлен пакет `popularity-contest`, то вы можете использовать команду **popcon-largest-unused** для получения списка неиспользуемых пакетов, которые занимают больше всего места. Вы можете найти пакеты, которые занимают больше всего дискового пространства с помощью **dpigs** (из пакета `debian-goodies`) или **wajig** (запустив `wajig size`). Также вы можете получить список пакетов, которые занимают больше всего места, с помощью **aptitude**. Запустите **aptitude** в режиме полнофункционального терминала, выберите Окна → Новый плоский список пакетов, нажмите **I** и введите `~i`, нажмите **S** и введите `~installsize`. После этого вы получите удобный список, с которым можете поработать.
- Удалить переводы и файлы локализации из системы, если они ненужны. Вы можете установить и настроить пакет `localepurge`, который поможет удалить неиспользуемые системные локали. Это сократит использование дискового пространства в `/usr/share/locale`.
- Временно перенести на другую машину или удалить системные журналы из `/var/log/`.

- Использовать временный каталог `/var/cache/apt/archives`: вы можете использовать временный каталог под кэш на другой файловой системе (USB-носителе, временно подключённом жёстком диске, уже используемой файловой системе, ...).

ЗАМЕЧАНИЕ

Не используйте файловые системы NFS, так как при обновлении могут возникнуть перебои в работе сети.

Например, если у вас есть USB-диск, смонтированный в `/media/usbkey`:

1. Удалите пакеты, которые были скачаны при установке ранее:

```
# apt clean
```

2. Скопируйте каталог `/var/cache/apt/archives` на USB-диск:

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

3. Смонтируйте временный каталог кэша:

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

4. После обновления восстановите оригинальный каталог `/var/cache/apt/archives`:

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

5. Удалите оставшийся `/media/usbkey/archives`.

Можно создать временный каталог кэша в любой файловой системе, уже смонтированной в системе.

- Выполнить минимальное обновление системы (см. Раздел 4.4.4) или частичное обновление, а затем полное обновление. После частичного обновления можно очистить кэш пакетов и приступить к полному обновлению.

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

4.4.4 Минимальное обновление системы

ВАЖНО

If you are upgrading remotely, be aware of Раздел 5.1.23.

В некоторых случаях выполнение сразу полного обновления (как описано далее) может привести к удалению большого числа пакетов, которые вы хотите оставить. Поэтому мы рекомендуем производить обновление в две стадии — сначала минимальное обновление, чтобы разобраться с конфликтами, а затем полное обновление, как описано в Раздел 4.4.5.

Для этого сначала выполните:

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

Это приведёт к обновлению только тех пакетов, которые можно обновить без необходимости удаления или установки других пакетов.

Минимальное обновление системы также может оказаться полезным, если в системе мало свободного места и полное обновление запустить из-за этого невозможно.

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 Обновление системы

После выполнения предыдущих шагов теперь можно приступить, собственно, к обновлению. Выполните команду:

```
# apt full-upgrade
```

Эта команда произведёт полное обновление системы, установив последние доступные версии всех пакетов и разрешив всех изменившиеся между выпусками зависимости. При необходимости будут установлены новые пакеты (обычно, это новые версии библиотек или переименованные пакеты) и удалены все вызывающие конфликты устаревшие пакеты.

При обновлении с набора компакт-дисков, DVD или дисков Blu-ray система несколько раз попросит вас вставить в привод соответствующий диск. Возможно, вам придётся вставлять один и тот же диск несколько раз. Это вызвано тем, что взаимосвязанные пакеты могут находиться на разных дисках.

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 Возможные проблемы во время обновления

В следующем разделе описаны известные проблемы, которые могут возникнуть при обновлении до bullseye.

4.5.1 Dist-upgrade завершается с ошибкой «Could not perform immediate configuration»

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 Ожидаемые удаления

В процессе обновления до bullseye может потребоваться удалить пакеты в системе. Точный список пакетов будет зависеть от набора установленных в системе пакетов. В данном документе даны общие советы об удалении, но если у вас имеются сомнения, то перед тем как продолжить, рекомендуется проверить все пакеты, которые предлагаются к удалению. Дополнительную информацию об устаревших пакетах в bullseye см. в Раздел 4.8.

4.5.3 Конфликты или заикливание в требованиях предварительной установки

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
```

чтобы удалить «проблемные» пакеты или

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

В чрезвычайных случаях вам может потребоваться принудительная переустановка командой типа

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

4.5.4 Файловые конфликты

При обновлении с «чистого» buster конфликтов файлов быть не должно, но они вполне возможны, если у вас установлены неофициальные адаптации (backports). При конфликте файлов появляются ошибки:

```
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>
```

Конфликт файлов можно попытаться разрешить принудительным удалением пакета, указанного в *последней* строке сообщения об ошибке:

```
# 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 Изменение настроек

Во время обновления система будет задавать вопросы о настройке или перенастройке некоторых пакетов. Если вас спросят, нужно ли заменить какой-то файл в каталоге `/etc/init.d` или `/etc/manpath.config`, версией, предоставленной сопровождающим пакета, обычно следует ответить «да», поскольку иначе будет нарушена целостность системы. Вы всегда сможете вернуть старые настройки, потому что предыдущие файлы настройки будут сохранены с расширением `.dpkg-old`.

Если вы не знаете, что делать, запишите имя пакета или файла и разберитесь с проблемой позднее. Информацию, выведившуюся на экран во время обновления, вы сможете найти в файле записи программы `script`.

4.5.6 Изменение консоли сеанса

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.

Чтобы восстановить консоль, на которой запущено обновление, нажмите `Ctrl+Alt+F1` для перехода обратно на виртуальный терминал 1 (если вы видите графический экран входа в систему) или используйте `Alt+F1` (если вы видите локальную консоль в текстовом режиме). Вместо `F1` нажмите функциональную клавишу с номером виртуального терминала, в котором запущено обновление. Также вы можете использовать `Alt+стрелка влево` или `Alt+стрелка вправо` для переключения между терминалами в текстовом режиме.

4.6 Обновление ядра и сопутствующих пакетов

В этом разделе описано как обновить ядро и указаны потенциальные проблемы, связанные с этим. Вы можете установить один из пакетов `linux-image-*`, предоставленных Debian, или скомпилировать ядро из исходного кода самостоятельно.

Заметим, что большая часть информации раздела основана на предположении, что вы будете использовать одно из модульных ядер Debian вместе с `initramfs-tools` и `udev`. Если вы будете использовать своё собственное ядро, которому не требуется `initrd`, или вы используете другой генератор `initrd`, то некоторая информация может быть для вас несущественна.

4.6.1 Установка метапакета ядра

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
```

Если в результате вы ничего не увидели, то вам нужно установить новый пакет `linux-image` вручную, либо установить метапакет `linux-image`. Чтобы увидеть список доступных метапакетов `linux-image`, выполните:

```
# 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 Раздел 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 Раздел 4.4.4.

4.7 Подготовка к следующему выпуску

Для подготовки к следующему выпуску после обновления можно сделать несколько вещей.

- Удалите устаревшие и неиспользуемые пакеты, как это описано в Раздел 4.4.3 и Раздел 4.8. Проверьте, какие файлы настроек они использовали и подумайте над вычисткой пакетов вместе с их файлами настройки. Также см. Раздел 4.7.1.

4.7.1 Вычистка удалённых пакетов

Как правило, рекомендуется вычистить удалённые пакеты. Это особенно справедливо в случае, если они были удалены при обновлении более раннего выпуска (напр., при обновлении до buster), или если они были предоставлены третьими лицами. В частности, старые сценарии `init.d` могут вызывать проблемы.

ПРЕДОСТЕРЕЖЕНИЕ



Вычищение пакетов, как правило, приводит также и к вычищению файлов журналов, возможно вам потребуется сделать их резервные копии.

Следующие команды отображают список всех удалённых пакетов, чьи файлы настройки всё ещё остаются в системе (если таковые имеются):

```
# 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 }')
```

Если вы используете `aptitude`, вы можете использовать следующие альтернативы приведённым выше командам:

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

4.8 Устаревшие пакеты

Вместе с появлением множества новых пакетов, из bullseye было удалено довольно много пакетов, которые входили в buster. Для таких устаревших пакетов возможности обновления нет. Ничто не мешает вам продолжать пользоваться устаревшими пакетами, но приблизительно через год после выхода bullseye Проект Debian обычно прекращает выпускать для них исправления безопасности⁵, и оказывать другую своевременную поддержку. Рекомендуется заменить их на доступные альтернативные пакеты (если таковые имеются).

Пакет может быть удалён из дистрибутива по многим причинам: разработка программы прекращена, пакет неинтересен никому из разработчиков Debian, программа вытеснена другой, более функциональной программой или версией программы, пакет содержит ошибки, из-за которых пока не может быть включён в bullseye. В последнем случае пакет может быть доступен в «нестабильной» ветви дистрибутива.

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

⁵Или при появлении нового выпуска Debian. Обычно поддержку получают одновременно не более двух стабильных выпусков.

category «Obsolete and Locally Created Packages», and they can be listed and purged from the commandline with:

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

В **системе отслеживания ошибок Debian** (<https://bugs.debian.org/>) зачастую содержится дополнительная информация о причинах удаления пакета. Просмотрите архив сообщений об ошибках интересующего вас пакета, а также архивированные ошибки на **псевдо-пакет ftp.debian.org** (<https://bugs.debian.org/cgi-bin/pkgreport.cgi?pkg=ftp.debian.org&archive=yes>).

Список устаревших пакетов для выпуска Bullseye можно посмотреть в Раздел **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 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.

Глава 5

Что нужно знать о bullseye

Иногда изменения, внесённые в новый выпуск, приводят к побочным эффектам, которых нельзя избежать без появления ошибок где-то ещё. Этот раздел описывает проблемы, которые уже известны нам. Прочитайте также список известных ошибок, соответствующую документацию на пакеты, отчёты об ошибках и другую информацию, указанную в Раздел 6.1.

5.1 Конкретные шаги обновления для bullseye

В данном разделе описываются шаги обновления с buster до 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 Раздел 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 Раздел [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 Глава [4](#), packages depending on `fuse3` might be kept back during upgrades. Running the steps discussed in Раздел [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/410a6ce5c80dd981c22752da034f2529b5e) (<https://github.com/fail2ban/fail2ban/commit/410a6ce5c80dd981c22752da034f2529b5e>) (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 То, что следует сделать после обновления и до перезагрузки

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 Ограничения поддержки безопасности

Для некоторых пакетов Debian не может гарантировать какой-либо минимальной поддержки исправлений безопасности. О таких пакетах написано в следующих разделах.

ЗАМЕЧАНИЕ



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` engines¹ are included in bullseye, but not covered by security support. These browsers should not be used against untrusted websites. The `webkit2gtk` and `wpewebkit` engines *are* covered by security support.

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

5.2.1.2 OpenJDK 17

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

5.2.1.3 Go-based packages

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

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

5.2.2 Accessing GNOME Settings app without mouse

Without a pointing device, there is no direct way to change settings in the GNOME Settings app provided by `gnome-control-center`. As a work-around, you can navigate from the sidebar to the main content by pressing the **Right Arrow** twice. To get back to the sidebar, you can start a search with `Ctrl + F`, type

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

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 Заслуживающие внимания устаревшие пакеты

Ниже приводится список заслуживающих внимания устаревших пакетов (описание см. в Раздел [4.8](#)).

В список устаревших пакетов входят следующие пакеты:

- 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 userland packages `isdnutils`, `isdnactivecards`, `drdsl` and `ibod` have been removed from the archives.
- The deprecated `libappindicator` libraries are no longer provided. As a result, the related packages `libappindicator1`, `libappindicator3-1` and `libappindicator-dev` are no longer available. This is expected to cause dependency errors for third-party software that still depends on `libappindicator` to provide system tray and indicator support.
Debian is using `libayatana-appindicator` as the successor of `libappindicator`. For technical background see [this announcement](https://lists.debian.org/debian-devel/2018/03/msg00506.html) (<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 Устаревшие компоненты bullseye

В следующем выпуске Debian 12 (кодовое имя `bookworm`) некоторые возможности устарели. Пользователям требуется перейти на использование других альтернатив, чтобы избежать проблем с обновлением до Debian 12.

Изменения коснулись следующих возможностей:

- 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>), `slapd-hdb(5)` (<https://manpages.debian.org//bullseye/slapd/slapd-hdb.5.html>), and `slapd-shell(5)` (<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>) backend.

Additionally, the `slapd-perl(5)` (<https://manpages.debian.org//bullseye/slapd/slapd-perl.5.html>) and `slapd-sql(5)` (<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 |
|---|-----------------------------|---|
| 922981 (https://bugs.debian.org/922981) | ca-certificates-java | ca-certificates-java: /etc/ca-certificates/update.d/jks-keystore doesn't update /etc/ssl/certs/java/cacerts |
| 990026 (https://bugs.debian.org/990026) | cron | cron: Reduced charset in MAILTO causes breakage |
| 991081 (https://bugs.debian.org/991081) | gir1.2-diodon-1.0 | gir1.2-diodon-1.0 lacks dependencies |
| 990318 (https://bugs.debian.org/990318) | python-pkg-resources | python-pkg-resources: please add Breaks against the unversioned python packages |
| 991449 (https://bugs.debian.org/991449) | fail2ban | fix for CVE-2021-32749 breaks systems with mail from bsd-mailx |
| 990708 (https://bugs.debian.org/990708) | mariadb-server-10.5, galera | mariadb-server-10.5: upgrade problems due to galera-3 -> galera-4 switch |
| 980429 (https://bugs.debian.org/980429) | src:gcc-10 | g++-10: spurious c++17 mode segmentation fault in append_to_statement_list_1 (tree-iterator.c:65) |
| 980609 (https://bugs.debian.org/980609) | src:gcc-10 | missing i386-cpuinfo.h |
| 984574 (https://bugs.debian.org/984574) | gcc-10-base | gcc-10-base: please add Breaks: gcc-8-base (< 8.4) |
| 984931 (https://bugs.debian.org/984931) | git-el | git-el,elpa-magit: fails to install: /usr/lib/emacsen-common/packages/install/git emacs failed at /usr/lib/emacsen-common/lib.pl line 19, <TSORT> line 7. |
| 987264 (https://bugs.debian.org/987264) | git-el | git-el: fails to install with xemacs21 |
| 991082 (https://bugs.debian.org/991082) | gir1.2-gtd-1.0 | gir1.2-gtd-1.0 has empty Depends |
| 948739 (https://bugs.debian.org/948739) | gpated | gpated should not mask .mount units |
| 984714 (https://bugs.debian.org/984714) | gpated | gpated should suggest exfatprogs and backport the commit that rejects exfat-utils |
| 984760 (https://bugs.debian.org/984760) | grub-efi-amd64 | grub-efi-amd64: upgrade works, boot fails (error: symbol `grub_is_lockdown` not found) |
| 968368 (https://bugs.debian.org/968368) | ifenslave | ifenslave: Option bond-master fails to add interface to bond |
| 990428 (https://bugs.debian.org/990428) | ifenslave | ifenslave: Bonding not working on bullseye (using bond-slaves config) |
| 991113 (https://bugs.debian.org/991113) | libpam-chroot | libpam-chroot installs pam_chroot.so into the wrong directory |
| 989545 (https://bugs.debian.org/989545) | 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 |
|---|----------------------------|--|
| 982459 (https://bugs.debian.org/982459) | mdadm | mdadm --examine in chroot without /proc,/dev,/sys mounted corrupts host's filesystem |
| 981054 (https://bugs.debian.org/981054) | openipmi | openipmi: Missing dependency on kmod |
| 948318 (https://bugs.debian.org/948318) | openssh-server | openssh-server: Unable to restart sshd restart after upgrade to version 8.1p1-2 |
| 991151 (https://bugs.debian.org/991151) | procps | procps: dropped the reload option from the init script, breaking corekeeper |
| 989103 (https://bugs.debian.org/989103) | pulseaudio | pulseaudio regressed on control = Wave configuration |
| 984580 (https://bugs.debian.org/984580) | libpython3.9-dev | libpython3.9-dev: missing dependency on zlib1g-dev |
| 990417 (https://bugs.debian.org/990417) | src:qemu | openjdk-11-jre-headless: running java in qemu s390 gives a SIGILL at C [linux-vdso64.so.1 + 0x6f8] _kernel_getcpu + 0x8 |
| 859926 (https://bugs.debian.org/859926) | speech-dispatcher | breaks with pulse-audio as output when spawned by speechd-up from init system |
| 932501 (https://bugs.debian.org/932501) | src:squid-deb-proxy | squid-deb-proxy: daemon does not start due to the conf file not being allowed by apparmor |
| 991588 (https://bugs.debian.org/991588) | tpm2-abrmd | tpm2-abrmd should not use Requires = systemd-udev-settle.service in its unit |
| 991939 (https://bugs.debian.org/991939) | libjs-bootstrap4 | libjs-bootstrap4: broken symlinks: /usr/share/javascript/bootstrap4/css/bootstrap*.css -> ../../../../nodejs/bootstrap/dist/css/bootstrap*.css.map |
| 991822 (https://bugs.debian.org/991822) | src:wine | src:wine: dh_auto_clean deletes unrelated files outside of package source |
| 988477 (https://bugs.debian.org/988477) | src:xen | xen-hypervisor-4.14-amd64: xen dmesg shows (XEN) AMD-Vi: IO_PAGE_FAULT on sata pci device |
| 991788 (https://bugs.debian.org/991788) | xfce4-settings | xfce4-settings: black screen after suspend when laptop lid is closed and re-opened |

Глава 6

Дополнительная информация о Debian

6.1 Что ещё можно прочитать

Помимо этой информации о выпуске и руководства по установке, существует документация по Debian, разрабатываемая проектом документирования Debian (DDP), целью которого является создание высококачественной документации для пользователей и разработчиков Debian. В состав этой документации входит справочник Debian, руководство нового сопровождающего Debian, ЧАВО по Debian и многое другое. Полную информацию о доступной документации можно посмотреть на [веб-сайте проекта документирования Debian](https://www.debian.org/doc/) (<https://www.debian.org/doc/>) и [Debian Wiki](https://wiki.debian.org/) (<https://wiki.debian.org/>).

Документация по конкретным пакетам устанавливается в каталог `/usr/share/doc/пакет`. Там может находиться информация об авторских правах, специфичная для Debian информация и документация из основной ветки разработки.

6.2 Если нужна помощь

Пользователи Debian могут воспользоваться помощью, советами и поддержкой из разных источников, но к ним следует прибегать только в том случае, если вам не удалось найти ответа в доступной документации. Данный раздел содержит краткое описание дополнительных источников помощи, которые могут оказаться полезными для новых пользователей Debian.

6.2.1 Списки рассылки

Основной интерес для пользователей Debian представляют англоязычный список рассылки `debian-user`, или списки `debian-user-язык` и `debian-язык` для других языков. Для русского языка это список `debian-russian`. Информацию о списках рассылки и о том как на них подписаться см. на <https://lists.debian.org/>. Пожалуйста, перед тем, как отправить вопрос в список рассылки, поищите ответ на него в архивах. Просим также придерживаться общепринятых норм почтового этикета.

6.2.2 IRC

Для поддержки пользователей Debian есть IRC-канал, размещённый в IRC-сети OFTC. Чтобы войти на канал, соединитесь с сервером `irc.debian.org` с помощью своего любимого IRC-клиента и присоединитесь к каналу `#debian`. Для русскоязычных пользователей существует канал `#debian-russian` в той же сети.

Просим вас следовать правилам поведения на канале и уважать других пользователей. Правила поведения на канале описаны в [вики Debian](https://wiki.debian.org/DebianIRC) (<https://wiki.debian.org/DebianIRC>).

Более подробную информацию об OFTC можно получить на [веб-сайте сети](http://www.oftc.net/) (<http://www.oftc.net/>).

6.3 Как сообщить об ошибке

Мы приложили немало усилий, чтобы сделать Debian операционной системой высокого качества, однако это не означает, что поставляемые нами пакеты совсем не содержат никаких ошибок. Такой подход согласуется с философией «открытой разработки» Debian. Мы предоставляем нашим пользователям полную информацию обо всех обнаруженных ошибках с помощью нашей системы отслеживания ошибок (BTS). Вы можете обратиться к ней по адресу <https://bugs.debian.org/>.

Если вы обнаружите ошибку в дистрибутиве или каком-то из его пакетов, пожалуйста, сообщите о ней, чтобы в будущих выпусках она была исправлена. Чтобы сообщить об ошибке, требуется рабочий адрес электронной почты. Это необходимо для того, чтобы мы могли отслеживать ошибки, а разработчики могли связываться с отправителями отчётов об ошибках, если им понадобится дополнительная информация.

Отправить сообщение об ошибке можно с помощью программы **reportbug** или вручную по электронной почте. Более подробную информацию о системе отслеживания ошибок и о том, как её использовать, можно прочитать в справочной документации (она доступна в каталоге `/usr/share/doc/debian` после установки пакета `doc-debian`) или на сайте **системы отслеживания ошибок** (<https://bugs.debian.org/>).

6.4 Как помочь Debian

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.

Если вы можете уделить Debian больше времени, можно взяться за сопровождение какой-нибудь свободной программы Free Software. В частности, полезной была бы поддержка пакетов, которые кто-то особенно хотел бы видеть в Debian. Подробную информацию можно найти на странице **требующих доработки и планируемых пакетов** (<https://www.debian.org/devel/wpp/>). Если вам интересна какая-то специфическая группа пользователей, возможно, вы захотите участвовать в одном из **дочерних проектов** (<https://www.debian.org/devel/#projects>) Debian. Среди них перенос Debian на другие архитектуры и **Debian Pure Blends** (<https://wiki.debian.org/DebianPureBlends>).

В любом случае, если вы участвуете в работе сообщества Свободного ПО в качестве пользователя, программиста, писателя или переводчика, вы уже помогаете Свободному программному обеспечению. Такое участие приносит удовольствие и радость, а также даёт возможность познакомиться с новыми людьми и придаёт вам те самые тёплые чувства и переживания.

Глава 7

Глоссарий

ACPI

усовершенствованный интерфейс настройки и управления питанием

ALSA

передовая звуковая архитектура Linux

BD

диск Blu-ray

CD

компакт-диск

CD-ROM

доступный только для чтения компакт-диск

DHCP

протокол динамической конфигурации узла

DLBD

двухслойный диск Blu-ray

DNS

система доменных имён

DVD

цифровой многоцелевой диск

GIMP

растровый графический редактор GNU

GNU

GNU не Unix

GPG

свободная альтернатива набору криптографического ПО PGP

LDAP

облегчённый протокол доступа к каталогам

LSB

набор стандартов Linux

LVM

менеджер логических томов

MTA

агент пересылки почты

NBD

сетевое блочное устройство

NFS

сетевая файловая система

NIC

плата сетевого интерфейса

NIS

сетевая информационная служба

PHP

PHP: препроцессор гипертекста

RAID

избыточный массив независимых жёстких дисков

SATA

присоединение по продвинутой технологии по последовательному интерфейсу

SSL

уровень защищённых сокетов

TLS

защищённый транспортный уровень

UEFI

Unified Extensible Firmware Interface (Унифицированный расширяемый интерфейс микропрограмм)

USB

универсальная последовательная шина

UUID

универсальный уникальный идентификатор

WPA

защищённый доступ к Wi-Fi

Приложение А

Подготовка системы **buster** к обновлению

В этом приложении содержится информация о том, как перед обновлением до bullseye удостовериться, что вы можете устанавливать или обновлять пакеты **buster**. Это может понадобиться в некоторых случаях.

А.1 Обновление системы **buster**

В основном, это обновление ничем не отличается от всех предыдущих обновлений **buster**, которые вы делали. Единственное отличие состоит в том, что сначала надо убедиться, что ваши списки пакетов всё ещё содержат ссылки на пакеты **buster**, как описано в Раздел [А.2](#).

Если вы обновляете систему с сервера-зеркала Debian, то автоматически будет выполнено обновление до последнего выпуска **buster**.

А.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.

Если вы успели установить пакеты из bullseye, то особого смысла в установке пакетов из **buster** уже нет. В этом случае вам следует решить — доводить до конца обновление или нет. Вернуться к использованию старых версий пакетов возможно, но эта процедура выходит за рамки данного документа.

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.

ВАЖНО



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.

Если вы внесли какие-нибудь изменения, сохраните файл и выполните команду

```
# apt update
```

для обновления списка пакетов.

А.3 Удаление устаревших файлов настройки

Перед обновлением системы до bullseye, рекомендуется удалить из системы старые файлы настроек (такие как *.dpkg-*{new, old}* в /etc).

Приложение В

Люди, участвовавшие в создании информации о выпуске

Много людей помогало при создании информации о выпуске, вот только некоторые из них:

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-Plić, 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 и W. Martin Borgert.

Этот документ был переведён на многие языки. Спасибо переводчикам!

Перевод на русский: Сергей Алёшин, Юрий Козлов, Лев Ламберов

Предметный указатель

A

Apache, 5

B

BIND, 5

C

Calligra, 3

Cryptsetup, 5

D

DocBook XML, 2

Dovecot, 5

E

Exim, 5

G

GCC, 5

GIMP, 5

GNOME, 3

GNUCash, 4

GnuPG, 5

I

Inkscape, 5

K

KDE, 3

L

LibreOffice, 3

LXDE, 3

LXQt, 3

M

MariaDB, 5

MATE, 3

N

Nginx, 5

O

OpenJDK, 5

OpenSSH, 5

P

packages

apt, 2, 16, 29

apt-listchanges, 21

aptitude, 14, 19, 24

aufs-dkms, 34

bsd-mailx, 31

ca-certificates-java, 35

chef, 33

cinder-volume, 28

connman, 34

cron, 35

cups-browsed, 5

cups-daemon, 5

cups-filters, 5

dblatex, 2

debian-goodies, 19

debian-kernel-handbook, 23

debian-security-support, 32

doc-debian, 38

docbook-xsl, 2

dpkg, 2

drdsl, 33

exfat-fuse, 6

exfat-utils, 7

exfatprogs, 7

fail2ban, 31, 35

firmware-iwlwifi, 31

fuse, 29

fuse3, 29

gcc-10-base, 35

gir1.2-diodon-1.0, 35

gir1.2-gtd-1.0, 35

git-el, 35

glibc, 28

gnome-control-center, 32

gparted, 35

grub-efi-amd64, 35

grub2, 33

guile-2.2-libs, 31

gvfs-fuse, 29

how-can-i-help, 38

i965-va-driver, 27

ibod, 33

ifenslave, 35

initramfs-tools, 12, 23

intel-media-va-driver, 27

intel-microcode, 31

ipp-usb, 5, 6

isdnactivecards, 33

isdnutils, 33

kio-fuse, 29

libappindicator-dev, 33

libappindicator1, 33

libappindicator3-1, 33

libayatana-appindicator, 33

libgc1c2, 31

libjs-bootstrap4, 36

libnss-nis, 28

libnss-nisplus, 28

libpam-chroot, 35

libpython3.9-dev, 36

libsane1, 5, 6

lilo, 33

linux-image-*, 23

linux-image-amd64, 23

linux-source, 23

localepurge, 19

mailman, 33
mailman3, 33
mailman3-full, 33
mailutils, 31
mariadb-server-10.5.galera-4, 35
mdadm, 36
network-manager, 34
nova-compute, 28
openipmi, 36
openssh-server, 31, 36
openvswitch, 31
popularity-contest, 19
procps, 36
pulseaudio, 36
python-pkg-resources, 35
python-setuptools, 34
rails, 30
rdiff-backup, 31
redmine, 30
release-notes, 1
rsync, 28
rsyslog, 6
sane-airscan, 5
sendmail, 29
slapd, 34
speech-dispatcher, 36
src:gcc-10, 35
src:llvm-toolchain-11, 35
src:qemu, 36
src:squid-deb-proxy, 36
src:wine, 36
src:xen, 36
sshfs, 29
synaptic, 14
systemd, 7
tinc, 13
tpm2-abrmd, 36
udev, 23, 30
unbound, 28
upgrade-reports, 1
usrmerge, 34
va-driver-all, 27
vim, 28
vim-addon-manager, 28
vim-scripts, 28
wicd, 34
xfce4-settings, 36
xmlroff, 2
xsltproc, 2

Perl, 5
PHP, 5
Postfix, 5
PostgreSQL, 5

X
Xfce, 3