

Poznámky k vydaniu Debian 11 (bullseye), 64-bit little-endian PowerPC

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

17. apríla 2024

Poznámky k vydaniu Debian 11 (bullseye), 64-bit little-endian PowerPC

Tento dokument je slobodný softvér; môžete ho šíriť a/alebo meniť za podmienok licencie GNU General Public License verzie 2 ako ju publikovala Free Software Foundation.

Tento program je šírený vo viere, že bude užitočný, ale BEZ AKEJKOLIEK ZÁRUKY; dokonca aj bez implicitnej záruky OBCHODOVATELNOSTI či VHODNOSTI NA URČITÝ ÚČEL. Podrobnosti nájdete v GNU General Public License.

Spolu s týmto programom by ste mali dostať kópiu GNU General Public License; ak nie, napíšte na adresu 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.

Obsah

1	Úvod	1
1.1	Ako oznamovať chyby v tomto dokumente	1
1.2	Ako posilať správy o aktualizácii	1
1.3	Zdroje tohto dokumentu	2
2	Čo je nové v Debian 11	3
2.1	Podporované architektúry	3
2.2	Čo je nové v distribúcii?	3
2.2.1	Desktops and well known packages	3
2.2.2	Driverless scanning and printing	4
2.2.2.1	CUPS and driverless printing	4
2.2.2.2	SANE and driverless scanning	4
2.2.3	New generic open command	5
2.2.4	Control groups v2	5
2.2.5	Persistent systemd journal	5
2.2.6	New Fcitx 5 Input Method	5
2.2.7	Novinky od Debian Med Blend	5
2.2.8	Kernel support for exFAT	5
2.2.9	Improved man page translations	6
2.2.10	Improved support for alternative init systems	6
2.2.11	Initial availability of the Bazel build system	6
3	Inštalčný systém	7
3.1	Čo je nové v inštalčnom systéme?	7
3.1.1	Help with installation of firmware	7
3.1.2	Automatizovaná inštalácia	7
3.2	Cloud installations	8
3.3	Container and Virtual Machine images	8
4	Aktualizácie z Debian 10 (buster)	9
4.1	Príprava na aktualizáciu	9
4.1.1	Zálohujte všetky dáta a konfiguračné údaje	9
4.1.2	Vopred informujte používateľov	9
4.1.3	Pripravte sa na odstávku služieb	9
4.1.4	Pripravte sa na obnovu	10
4.1.4.1	Ladiaci shell počas štartu pomocou initrd	10
4.1.4.2	Ladiaci shell počas štartu pomocou systemd	10
4.1.5	Pripravte bezpečné prostredie na aktualizáciu	11
4.2	Start from “pure” Debian	11
4.2.1	Upgrade to Debian 10 (buster)	11
4.2.2	Remove non-Debian packages	11
4.2.3	Upgrade to latest point release	11
4.2.4	Prepare the package database	12
4.2.5	Remove obsolete packages	12
4.2.6	Clean up leftover configuration files	12
4.2.7	The security section	12
4.2.8	Sekcia proposed-updates	12
4.2.9	Neoficiálne zdroje	12
4.2.10	Vypnite pripevňovanie balíkov APT (APT pinning)	12
4.2.11	Check package status	13
4.3	Preparing APT source-list files	13
4.3.1	Pridávanie internetových zdrojov APT	14
4.3.2	Pridanie zdrojov APT lokálneho zrkadla	14
4.3.3	Pridanie zdrojov APT z optických médií	14

4.4	Aktualizácia balíkov	15
4.4.1	Nahrание relácie príkazového riadka	15
4.4.2	Aktualizácia zoznamu balíkov	16
4.4.3	Uistite sa, že na aktualizáciu máte dosť miesta na disku	16
4.4.4	Minimálna aktualizácia systému	18
4.4.5	Aktualizácia systému	18
4.5	Možné problémy počas aktualizácie	18
4.5.1	Dist-upgrade zlyhá s chybou „Nebolo možné vykonať okamžitú konfiguráciu“	18
4.5.2	Očakávané odstránenia	19
4.5.3	Cykly Konfliktov alebo Predzávislostí	19
4.5.4	Konflikty súborov	19
4.5.5	Zmeny v konfigurácii	19
4.5.6	Zmena relácie na konzolu	20
4.6	Aktualizácia jadra a súvisiacich balíkov	20
4.6.1	Inštalácia metabalíka jadra	20
4.7	Príprava na ďalšie vydanie	20
4.7.1	Vyčistenie (purge) odstránených balíkov	21
4.8	Zastaralé balíky	21
4.8.1	Transitional dummy packages	22
5	Problémy vyskytujúce sa v bullseye	23
5.1	Položky týkajúce sa aktualizácie na bullseye	23
5.1.1	The XFS file system no longer supports barrier/nobarrier option	23
5.1.2	Changed security archive layout	23
5.1.3	Password hashing uses yescrypt by default	23
5.1.4	NSS NIS and NIS+ support require new packages	24
5.1.5	Config file fragment handling in unbound	24
5.1.6	rsync parameter deprecation	24
5.1.7	Vim addons handling	24
5.1.8	OpenStack and cgroups v1	24
5.1.9	OpenStack API policy files	24
5.1.10	sendmail downtime during upgrade	25
5.1.11	FUSE 3	25
5.1.12	GnuPG options file	25
5.1.13	Linux enables user namespaces by default	25
5.1.14	Linux disables unprivileged calls to bpf() by default	25
5.1.15	redmine missing in bullseye	25
5.1.16	Exim 4.94	26
5.1.17	SCSI device probing is non-deterministic	26
5.1.18	rdiff-backup require lockstep upgrade of server and client	26
5.1.19	Intel CPU microcode issues	26
5.1.20	Upgrades involving libgc1c2 need two runs	27
5.1.21	fail2ban can't send e-mail using mail from BSD-mailx	27
5.1.22	No new SSH connections possible during upgrade	27
5.1.23	Open vSwitch upgrade requires interfaces(5) change	27
5.1.24	Čo urobiť po aktualizácii pred reštartom	27
5.2	Items not limited to the upgrade process	27
5.2.1	Obmedzenia bezpečnostnej podpory	27
5.2.1.1	Security status of web browsers and their rendering engines	28
5.2.1.2	OpenJDK 17	28
5.2.1.3	Go-based packages	28
5.2.2	Accessing GNOME Settings app without mouse	28
5.2.3	The rescue boot option is unusable without a root password	28
5.2.4	32-bit Xen PV guests are not supported	29
5.3	Obsolescence and deprecation	29
5.3.1	Významné zastaralé balíky	29
5.3.2	Zastaralé súčasti bullseye	30
5.4	Known severe bugs	30

6	Ďalšie informácie o Debiane	33
6.1	Ďalšie čítanie	33
6.2	Ako získať pomoc	33
6.2.1	Konferencie	33
6.2.2	Internet Relay Chat	33
6.3	Oznamovanie chýb	33
6.4	Ako prispievať do Debianu	34
7	Slovník	35
A	Ako spravovať váš systém buster pred aktualizáciou	37
A.1	Ako aktualizovať váš systém buster	37
A.2	Checking your APT source-list files	37
A.3	Odstránenie zastaralých konfiguračných súborov	38
B	Prispievatelia do Poznámok k vydaniu	39
	Register	41

Kapitola 1

Úvod

Tento dokument informuje používateľov distribúcie Debian o hlavných zmenách vo verzii 11 (kódové označenie „bullseye“).

Poznámky k vydaniu poskytujú informácie o tom ako bezpečne aktualizovať systém z predošlého vydania 10 (kódové označenie buster) na aktuálne vydanie a informujú používateľov o známych potenciálnych problémoch, s ktorými by sa mohli stretnúť počas aktualizácie.

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

VÝSTRAHA



Majte na pamäti, že nie je možné uviesť každý známy problém a preto boli tu uvedené problémy vybrané na základe očakávanej frekvencie výskytu a závažnosti.

Prosím, majte na pamäti, že aktualizácia je podporovaná a zdokumentovaná iba z predošlého vydania Debianu (v tomto prípade z vydania buster). Ak potrebujete vykonať aktualizáciu zo staršieho vydania, mali by ste si prečítať Poznámky k vydaniu predošlého vydania a najprv aktualizovať na buster.

1.1 Ako oznamovať chyby v tomto dokumente

Pokúsili sme sa otestovať všetky rozličné kroky aktualizácie popísané v tomto dokumente a tiež sme sa pokúsili predvídať všetky možné problémy, s ktorými sa naši používatelia môžu stretnúť.

Ak si napriek tomu myslíte, že ste našli akúkoľvek chybu (nesprávne alebo chýbajúce informácie) v tejto dokumentácii, prosím oznámte chybu do [systému sledovania chýb](https://bugs.debian.org/) (<https://bugs.debian.org/>) voči balíku `release-notes`. Najskôr si však pozrite [existujúce hlásenia o chybách](https://bugs.debian.org/release-notes) (<https://bugs.debian.org/release-notes>), pre prípad, že je chyba, ktorú oznamujete, už nahlásená. Pokojne pridajte ďalšie informácie k existujúcim hláseniam chýb ak si myslíte, že môžete poskytnúť obsah do tohto dokumentu.

Oceňujeme a posmeľujeme zadávanie hlásení so záplatami zdrojových súborov tohto dokumentu. Ďalšie informácie o tom ako získať zdrojové súbory tohto dokumentu popisuje Oddiel [1.3](#).

1.2 Ako posilať správy o aktualizácii

Vítané sú všetky informácie od používateľov, ktoré sa týkajú aktualizácie z buster na bullseye. Ak ste ochotný podeliť sa o tieto informácie, nahláste prosím chybu s vašimi výsledkami do [systému sledovania chýb](https://bugs.debian.org/) (<https://bugs.debian.org/>) voči balíku `upgrade-reports`. Žiadame, aby ste všetky prípadné prílohy skomprimovali (pomocou `gzip`).

Prosím, uveďte pri posielaní správ o aktualizácii nasledovné údaje:

- Stav vašej databázy balíkov pred a po aktualizácii: stavová databáza `dpkg` je dostupná v `/var/lib/dpkg/status` a stavová databáza `apt` je dostupná v `/var/lib/apt/extended_states`.

Pred aktualizáciou by ste mali vykonať zálohovanie ako popisuje Oddiel 4.1.1, ale zálohy `/var/lib/dpkg/status` môžete tiež nájsť vo `/var/backups`.

- Záznamy relácie pomocou príkazu `script` popisuje Oddiel 4.4.1 .
- Vaše záznamy `apt` dostupné v `/var/log/apt/term.log` alebo vaše záznamy `aptitude` dostupné v `/var/log/aptitude`.

POZNÁMKA



Pozn.: Mali by ste venovať nejaký čas tomu, aby ste skontrolovali, či spolu so záznamami neodosielate akékoľvek citlivé alebo dôverné informácie a odstrániť ich zo správy, pretože tieto informácie budú verejne prístupné.

1.3 Zdroje tohto dokumentu

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

Kapitola 2

Čo je nové v Debian 11

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

2.1 Podporované architektúry

Debian bullseye oficiálne podporuje nasledovné architektúry:

- 32-bitové PC (`i386`) a 64-bitové PC (`amd64`)
- 64-bitový ARM (`arm64`)
- ARM EABI (`armel`)
- ARMv7 (EABI hard-float ABI, `armhf`)
- little-endian MIPS (`mipsel`)
- 64-bitový little-endian PowerPC (`mips64el`)
- 64-bitový little-endian PowerPC (`ppc64el`)
- IBM System z (`s390x`)

Ďalšie informácie o stave portov a informácie špecifické pre vašu architektúru sa dočítate na [stránkach portov Debianu](https://www.debian.org/ports/) (<https://www.debian.org/ports/>).

2.2 Čo je nové v distribúcii?

Toto nové vydanie Debianu opäť prináša omnoho viac softvéru ako jeho predchodca buster; distribúcia obsahuje viac ako 11294 nových balíkov, čo je celkovo viac ako 59551 balíkov. Väčšina softvéru v distribúcii bola aktualizovaná: viac ako 42821 softvérových balíkov (to predstavuje 72 % všetkých balíkov v buster). Rovnako bolo z rôznych dôvodov z distribúcie odstránené významné množstvo balíkov (viac ako 9519, 16 % balíkov v buster). Neuvidíte žiadne aktualizácie týchto balíkov a v systémoch na správu balíkov budú označené ako „zastaralé“; pozri Oddiel [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.

Kancelárske aplikácie tiež boli aktualizované, vrátane kancelárskych balíkov:

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

Okrem množstva ďalších obsahuje toto vydanie aj nasledovné aktualizácie softvéru:

Balík	Verzia v 10 (buster)	Verzia v 11 (bullseye)
Apache	2.4.38	2.4.48
DNS server BIND	9.11	9.16
Cryptsetup	2.1	2.3
Dovecot MTA	2.3.4	2.3.13
Emacs	26.1	27.1
Predvolený emailový server Exim	4.92	4.94
GNU Compiler Collection ako štandardný kompilátor	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
knižnica GNU C	2.28	2.31
lighttpd	1.4.53	1.4.59
Obraz linuxového jadra	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
MTA Postfix	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 Oddiel 5.1.8 section.

2.2.5 Persistent systemd journal

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

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

2.2.6 New Fcix 5 Input Method

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

2.2.7 Novinky od Debian Med Blend

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>).

2.2.11 Initial availability of the Bazel build system

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

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

Kapitola 3

Inštaláčny systém

Inštalátor Debianu (Debian Installer) je oficiálny inštaláčny systém Debianu. Ponúka rôzne spôsoby inštalácie. Metódy inštalácie dostupné pre váš systém závisia na architektúre, ktorú používate.

Obrazy inštalátora pre bullseye nájdete spolu s Inštaláčnou príručkou na [webe Debianu](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/jazyk/index.html
```

Tiež si môžete pozrieť zoznam známych problémov s debian-installer - [errata](https://www.debian.org/releases/bullseye/debian-installer/index#errata) (<https://www.debian.org/releases/bullseye/debian-installer/index#errata>).

3.1 Čo je nové v inštaláčnom systéme?

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 Automatizovaná inštalácia

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.

[Inštaláčná príručka](https://www.debian.org/releases/bullseye/installmanual) (<https://www.debian.org/releases/bullseye/installmanual>) obsahuje samostatnú aktualizovanú prílohu s rozsiahlou dokumentáciou týkajúcou sa vopred zostavenej konfigurácie.

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>).

Kapitola 4

Aktualizácie z Debian 10 (buster)

4.1 Príprava na aktualizáciu

Odporúčame, aby ste si pred aktualizáciou prečítali aj informácie v časti Kapitola 5, ktorá pokrýva možné problémy nie priamo sa týkajúce procesu aktualizácie, ale o ktorých je dôležité vedieť predtým, než začnete.

4.1.1 Zálohujte všetky dáta a konfiguračné údaje

Dôrazne odporúčame, aby ste pred aktualizáciou systému vykonali úplnú zálohu alebo aspoň záložovali všetky dáta a konfiguračné údaje, ktoré si nemôžete dovoliť stratiť. Aktualizačné nástroje a proces aktualizácie sú dosť spoľahlivé, ale chyba hardvéru uprostred aktualizácie môže spôsobiť ťažké poškodenie systému.

Hlavné veci, ktoré budete chcieť zálohovať sú obsah `/etc`, `/var/lib/dpkg`, `/var/lib/aptitude/pkgstates` a výstup `dpkg --get-selections "*" (úvodzovky sú dôležité)`. Ak používate na správu balíkov vášho systému **aptitude**, budete si tiež chcieť zálohovať `/var/lib/aptitude/pkgstates`.

Samotný proces aktualizácie nemení nič v adresári `/home`. Ale niektoré aplikácie (napr. časti balíka Mozilla a pracovné prostredia GNOME a KDE) prepisujú existujúce nastavenia používateľa novými štandardnými hodnotami, keď používateľ prvýkrát spustí novú verziu aplikácie. Preventívne si môžete urobiť zálohu skrytých súborov a adresárov (súbory začínajúce bodkou) v domovských adresároch používateľov. Táto záloha môže pomôcť v obnovení alebo opätovnom vytvorení pôvodných nastavení. Tiež o tom môžete chcieť informovať používateľov.

Všetky operácie inštalácie balíkov musíte spúšťať s oprávnením superpoužívateľa, takže sa buď prihláste ako `root` alebo použite príkaz `su` alebo `sudo` na získanie potrebných oprávnení.

Aktualizácia má niekoľko predpokladov. Pred jej vykonaním by ste mali skontrolovať, či sú splnené.

4.1.2 Vopred informujte používateľov

Je rozumné informovať všetkých používateľov o plánovaných aktualizáciách, hoci používatelia prístupujú k systému pomocou `ssh` pripojenia by si toho počas aktualizácie nemuseli mnoho všimnúť a mali by byť schopní pokračovať v práci.

Ak si želáte vykonať ďalšie opatrenia, pred aktualizáciou zálohujte alebo odpojte `/home`.

Pri aktualizácii na bullseye budete musieť vykonať aktualizáciu jadra, takže bude potrebné reštartovať systém. Spravidla sa to robí po dokončení aktualizácie.

4.1.3 Pripravte sa na odstávku služieb

Vyšší systém môže ponúkať služby poskytované balíkmi, ktoré sa budú aktualizovať. V tom prípade, prosím, pamätajte, že počas aktualizácie budú služby zastavené, pokiaľ sa príslušné balíky nenahradia a nenakonfigurujú. V tejto dobe tieto služby nebudú dostupné.

Presná odstávka týchto služieb bude závisieť na počte balíkov systému, ktoré sa aktualizujú a predĺži sa tiež o čas, ktorý bude správca potrebovať na to, aby odpovedal na konfiguračné otázky od rôznych aktualizovaných balíkov (ak sa vyskytnú). Pamätajte, že ak necháte bežať proces aktualizácie bez dozoru

a systém bude počas aktualizácie požadovať vstup, je veľká pravdepodobnosť nedostupnosti služieb¹ po nezanedbateľnú dobu.

Ak systém, ktorý aktualizujete, poskytuje nevyhnutné služby pre vašich používateľov alebo siet², môžete čas odstávky znížiť vykonaním minimálnej aktualizácie systému ako popisuje Oddiel 4.4.4, následne aktualizáciou jadra a reštartom, a potom aktualizovať balíky súvisiace s vašimi nevyhnutnými službami. Aktualizáciu týchto balíkov pred vykonaním úplnej aktualizácie popisuje Oddiel 4.4.5. Takto môžete zabezpečiť, že tieto nevyhnutné služby pobežia a budú dostupné počas úplnej aktualizácie a tak sa zníži doba ich nedostupnosti.

4.1.4 Pripravte sa na obnovu

Hoci Debian sa snaží zabezpečiť, aby váš systém zostal po celú dobu v spustiteľnom stave, vždy existuje riziko, že po reštartovaní systému po aktualizácii môžete naraziť na problémy. Známe potenciálne problémy sú zdokumentované v tejto a ďalšej kapitole týchto Poznámok k vydaniu.

Z toho dôvodu sa uistite, že budete schopní obnoviť systém v prípade, že sa mu nepodarí znova naštartovať alebo, v prípade systémov spravovaných na diaľku, ak sa nepodarí aktivovať sieťové pripojenie.

Ak vykonávate vzdialenú aktualizáciu prostredníctvom spojenia **ssh**, odporúčame, aby ste vykonali nutné opatrenia, aby ste mali prístup k serveru prostredníctvom vzdialeného sériového terminálu. Existuje totiž možnosť, že po aktualizácii jadra a reštartovaní budete musieť opraviť konfiguráciu systému z lokálnej konzoly. Tiež v prípade, že sa systém náhodou uprostred aktualizácie reštartuje, existuje možnosť, že budete musieť opraviť konfiguráciu systému z lokálnej konzoly.

Na zotavenie v prípade núdze odporúčame vo všeobecnosti, aby ste použili *záchranný režim* inštalátora Debianu. Výhodou použitia inštalátora je, že si môžete vybrať medzi jeho mnohými spôsobmi inštalácie taký, ktorý sa najviac hodí vašej situácii. Ďalšie informácie nájdete v časti “Obnova poškodeného systému” v kapitole 8 *Inštaláčnej príručky* (<https://www.debian.org/releases/bullseye/installmanual>) a v *Často kladených otázkach k Inštalátoru Debianu* (<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 Ladiaci shell počas štartu pomocou initrd

Balík `initramfs-tools` obsahuje ladiaci shell³ v obrazoch `initrd`, ktoré generuje. Ak napríklad `initrd` nie je schopný pripojiť váš koreňový súborový systém, dostanete sa do tohto ladiaceho shellu, ktorý má základné príkazy na to, aby vám pomohol vystopovať problém a prípadne ho opraviť.

Základné veci, ktoré by ste mali skontrolovať: prítomnosť správnych súborov zariadení v `/dev`; aké moduly sú načítané (`cat /proc/modules`); chyby pri načítaní ovládačov vo výstupe **dmmsg**. Výstup príkazu **dmmsg** vám tiež ukáže ktoré súbory zariadení boli pridelené ktorým diskom; mali by ste si to overiť porovnaním s výstupom `echo $ROOT`, aby ste sa uistili, že koreňový systém je na zariadení, na ktorom ho očakávate.

Ak sa vám podarí opraviť problém, napísaním `exit` opustíte ladiaci shell a proces zavádzania bude pokračovať od bodu, kde bol prerušený. Samozrejme budete tiež musieť opraviť podstatu problému a znova vytvoriť `initrd`, aby nasledujúci štart už nezlyhal.

4.1.4.2 Ladiaci shell počas štartu pomocou systemd

Ak zavedenie systému pod `systemd` zlyhá, je root shell na ladenie získate zmenou príkazového riadka jadra. Ak zavedenie systému ako také uspeje, ale nepodarí sa spustiť niektoré služby, môže byť užitočné pridať k parametrom jadra `systemd.unit=rescue.target`.

¹Ak je priorita `debconf` nastavená na veľmi vysokú úroveň, môžete predísť konfiguračným výzvam, ale služby, ktoré na vašom systéme vyžadujú iné ako predvolené odpovede, sa nespustia.

²Napríklad: služby DNS alebo DHCP, obzvlášť ak bežia bez redundantného alebo záložného servera. V prípade DHCP sa môže stať, že budú používatelia odpojení od siete ak čas prenájmu ich IP adresy vyprší pred dokončením procesu aktualizácie.

³Túto vlastnosť možno vypnúť pridaním `panic=0` medzi parametre pri zavádzaní systému.

V opačnom vám prípade parameter jadra `systemd.unit=emergency.target` poskytne root shell v najbližšom možnom momente. Toto sa však deje pred pripojením koreňového súborového systému s povoleniami na čítanie aj zápis. To budete musieť urobiť ručne pomocou:

```
# 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 Pripravte bezpečné prostredie na aktualizáciu

DÔLEŽITÉ



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

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

4.2 Start from “pure” Debian

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

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

4.2.1 Upgrade to Debian 10 (buster)

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

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

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

4.2.2 Remove non-Debian packages

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

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

4.2.3 Upgrade to latest point release

This procedure assumes your system has been updated to the latest point release of buster. If you have not done this or are unsure, follow the instructions in Oddiel [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 Oddiel [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 Oddiel [5.1.2](#).

4.2.8 Sekcia 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 Neoficiálne zdroje

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.

Niektorí používatelia môžu používať *neoficiálne* spätne portované „novšie“ verzie balíkov, ktoré sú v Debiane nainštalované na ich systéme *buster*. Také balíky pravdepodobne spôsobia problémy počas aktualizácie, pretože môžu mať konfliktné súbory⁴. Oddiel [4.5](#) obsahuje informácie o tom, ako sa vyrovnáť s konfliktami ak nastanú.

4.2.10 Vypnite pripevňovanie balíkov APT (APT pinning)

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

⁴ Systém správy balíkov Debianu za bežných okolností neumožňuje balíku nahradiť súbor, ktorý vlastní iný balík, iba ak daný balík nahrádza tento vlastniaci balík.

4.2.11 Check package status

Bez ohľadu na použitú metódu aktualizácie sa odporúča, aby ste najskôr skontrolovali stav všetkých balíkov a overili, že sú v stave, aby sa dali aktualizovať. Nasledovný príkaz zobrazí všetky balíky, ktoré sú v stave „napoly inštalovaný“ alebo „konfigurácia zlyhala“ a všetky ostatné s chybovým stavom.

```
# dpkg --audit
```

Môžete tiež skontrolovať stav všetkých balíkov na vašom systéme pomocou **aptitude** alebo pomocou príkazov ako

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

alebo

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

Je žiaduce odstrániť pred aktualizáciou podržania. Ak je podržaný niektorý z dôležitých balíkov, ktoré sa majú aktualizovať, aktualizácia zlyhá.

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$'
```

Ak ste zmenili alebo prekompilovali balík lokálne a nepremenovali ste ho alebo ste dali do verzie epochu, musíte ho podržať, aby sa neaktualizoval.

The “hold” package state for **apt** can be changed using:

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

Stav balíka „podržať“ zrušíte nahradením príkazu `hold` príkazom `install`.

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 Oddiel 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.

Na vydanie je často možné odkazovať jednak prostredníctvom jeho kódového označenia (napr. `buster`, `bullseye`) a jednak jeho stavom (i.e. `oldstable`, `stable`, `testing`, `unstable`). Ak odkazujete na vydanie jeho kódovým označením má to tú výhodu, že vás nikdy neprekvapí nové vydanie a preto je to tu popísaný postup. To samozrejme tiež znamená, že budete musieť sledovať oznámenia o novom vydaní sami. Ak použijete namiesto kódového označenia stav, po vydaní uvidíte iba veľké množstvo aktualizácií balíkov.

Debian poskytuje dve poštové konferencie s oznámeniami, ktoré vás informujú o relevantných informáciách týkajúcich sa vydání Debianu.

- Po **príhlásení sa k odberu poštovej konferencie oznámení Debianu** (<https://lists.debian.org/debian-announce/>) budete dostávať oznámenie vždy, keď Debian uvoľní nové vydanie. Napr. keď sa `bullseye` zmení zo `testing` na `stable`.
- Po **príhlásení sa k odberu poštovej konferencie bezpečnostných oznámení** (<https://lists.debian.org/debian-security-announce/>) budete dostávať oznámenie vždy, keď Debian zverejní oznámenie týkajúce sa bezpečnosti.

4.3.1 Pridávanie internetových zdrojov 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).

Napríklad predpokladajme, že vaše najbližšie zrkadlo Debianu je `http://mirrors.kernel.org`. Keď sa na toto zrkadlo pozriete svojim webovým prehliadačom, všimnete si, že adresáre sú organizované nasledovne:

```
http://mirrors.kernel.org/debian/dists/bullseye/main/binary-ppc64el/...
http://mirrors.kernel.org/debian/dists/bullseye/contrib/binary-ppc64el/...
```

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
```

Všimnite si, že „dists“ sa pridáva implicitne a argumenty za názvom vydania sa použijú na doplnenie cesty o viaceré adresáre.

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

4.3.2 Pridanie zdrojov APT lokálneho zrkadla

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).

Napríklad, ak máte zrkadlo balíkov vo `/var/local/debian/` a adresárová štruktúra je nasledovná:

```
/var/local/debian/dists/bullseye/main/binary-ppc64el/...
/var/local/debian/dists/bullseye/contrib/binary-ppc64el/...
```

Pridaním nasledovného riadka do súboru `sources.list` ho môžete použiť v systéme apt:

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

Všimnite si, že „dists“ sa pridáva implicitne a argumenty za názvom vydania sa použijú na doplnenie cesty o viaceré adresáre.

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 Pridanie zdrojov APT z optických médií

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.

Uistite sa, že sa v súbore `/etc/fstab` nachádza riadok, ktorý umožňuje pripojiť vašu mechaniku CD-ROM na prípojný bod `/media/cdrom`. Napríklad, ak je vaša mechanika CD-ROM `/dev/sr0`, `/etc/fstab` by mal obsahovať takýto riadok:

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

Pamätajte, že medzi slovami `noauto,ro` v štvrtom poli nesmú byť žiadne medzery. Overte, že to funguje tak, že vložíte CD a skúsíte spustiť

```
# 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
```

Potom spustite:

```
# apt-cdrom add
```

pre každé binárne CD Debianu, ktoré máte, čím sa pridajú údaje o každom CD do databázy APT.

4.4 Aktualizácia balíkov

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

POZNÁMKA



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.

Nezabudnite pripojiť všetky potrebné diskové oblasti (predovšetkým koreňovú oblasť a oblasť obsahujúcu `/usr`) na zápis pomocou príkazu ako:

```
# 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.

POZNÁMKA



Riadky zdrojov softvéru týkajúce sa CD-ROM môžu niekedy odkazovať na „unstable“; a hoci to môže byť máťúce, *nemali* by ste to meniť.

4.4.1 Nahranie relácie príkazového riadka

Dôrazne sa odporúča použiť program `/usr/bin/script` na zaznamenanie priebehu relácie aktualizácie. Ak sa potom vyskytne problém, budete mať záznam toho, čo sa stalo a ak to bude potrebné, budete schopní poskytnúť presné informácie pri hlásení chyby. Zaznamenávanie spustíte príkazom:

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

alebo podobným. Ak budete musieť znova spustiť záznam (napr. ak musíte reštartovať systém), použijete inú hodnotu *krok* na rozlíšenie, ktorý krok aktualizácie zaznamenávate. Neukladajte súbor so záznamom do odkladacieho adresára ako `/tmp` či `/var/tmp` (súbory v týchto adresároch môžu byť počas aktualizácie alebo akéhokoľvek reštartu zmazané).

Záznam vám tiež umožní skontrolovať informácie, ktoré sa posunuli mimo obrazovky. Ak ste na konzole systému, stačí prepnúť na druhý virtuálny terminál (pomocou `Alt+F2`) a po prihlásení použijte na zobrazenie súboru `less -R ~root/upgrade-bullseye.script`.

Po dokončení aktualizácie môžete zastaviť **script** napísaním `exit` na príkazovom riadku.

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`.

Ak ste použili voľbu `-t` príkazu **script**, môžete použiť program **scriptreplay** na opätovné prehranie celej relácie:

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

4.4.2 Aktualizácia zoznamu balíkov

Najprv je potrebné stiahnuť zoznam dostupných balíkov nového vydania. To spravíte príkazom:

```
# apt update
```

POZNÁMKA



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 Uistite sa, že na aktualizáciu máte dosť miesta na disku

Pred aktualizáciou systému sa musíte uistiť, že máte dostatok miesta na disku než začnete úplnú aktualizáciu systému ako ju popisuje Oddiel 4.4.5. Všetky balíky potrebné na inštaláciu sa najprv stiahnu zo siete a uložia do adresára `/var/cache/apt/archives` (a počas sťahovania do podadresára `partial/`), takže sa musíte uistiť, že máte na oblasti, ktorá obsahuje `/var/` dostatok miesta na stiahnutie balíkov, ktoré sa budú inštalovať. Po stiahnutí pravdepodobne bude potrebné ďalšie miesto na disku v iných oblastiach na inštaláciu aktualizovaných balíkov (ktoré môžu obsahovať väčšie binárne súbory alebo viac dát) ako aj nových balíkov, ktoré sa stiahnu počas aktualizácie. Ak váš systém nebude mať dostatočné miesto na disku, môžete skončiť s neúplnou aktualizáciou, z čoho je ťažké systém zotaviť.

`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.
```

POZNÁMKA



Spustenie tohto príkazu na začiatku aktualizácie môže zobrazíť chybovú správu z dôvodov popísaných v ďalších častiach. V takom prípade budete musieť počkať, kým sa vykoná minimálna aktualizácia systému podľa Oddiel 4.4.4 a aktualizovať jadro pred spustením tohto príkazu na odhad miesta na disku.

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/.
```

V takejto situácii vopred uvoľnite miesto na disku. Môžete:

- 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
```

Na nájdenie zastaralých balíkov môžete tiež použiť **debfooster** alebo **cruft**. Nemali by ste balíky, ktoré vám tieto nástroje nájdu iba slepo odstraňovať, obzvlášť ak používate agresívne neštandardné voľby, ktoré často označia aj používané balíky. Dôrazne sa odporúča, aby ste manuálne skontrolovali balíky navrhnuté na odstránenie (t.j. ich obsah, veľkosť a popis) než ich necháte odstrániť.

- Odstráňte balíky, ktoré zaberajú príliš mnoho miesta a momentálne nie sú potrebné (po aktualizácii ich môžete vždy nainštalovať). Ak máte nainštalovaný `popularity-contest`, môžete použiť príkaz **popcon-largest-unused** na vypísanie zoznamu balíkov, ktoré nepoužívate a ktoré zaberajú najviac miesta. Balíky, ktoré len zaberajú najviac miesta na disku nájdete pomocou **dpigs** (dostupné v balíku `debian-goodies`) alebo **wajig** (príkazom `wajig size`). Tiež sa dajú nájsť pomocou `aptitude`. Spustíte **aptitude** v celobrazovkovom režime, vyberte Pohľad → Nový Plochý Zoznam Balíkov, stlačte **l** a zadajte `~i`, potom stlačte **S** a zadajte `~installsize`. To vám dá šikovný zoznam, s ktorým môžete ďalej pracovať.
- Odstrániť preklady a lokalizačné súbory zo systému, ak nie sú potrebné. Môžete nainštalovať balík `localepurge` a nastaviť ho, aby ponechal na systéme iba niekoľko vybraných locales. Tým sa zníži využitie miesta na disku, ktoré zaberá `/usr/share/locale`.
- Dočasne presunúť na iný systém alebo natrvalo odstrániť systémové záznamy nachádzajúce sa vo `/var/log/`.
- Použiť dočasný adresár `/var/cache/apt/archives`: Môžete použiť dočasný adresár pre vyrovnávaciu pamäť na inom súborovom systéme (USB pamäť, dočasný pevný disk, už používaný súborový systém, ...).

POZNÁMKA



Nepoužívajte prípojný bod NFS, pretože sieťové pripojenie sa môže počas aktualizácie prerušiť.

Napríklad, ak máte USB pamäť pripojenú na `/media/usbkey`:

1. odstráňte balíky, ktoré boli doteraz stiahnuté na inštaláciu:

```
# apt clean
```

2. skopírujte adresár `/var/cache/apt/archives` na USB pamäť:

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

3. pripojte dočasný adresár vyrovnávacej pamäte balíkov na aktuálny:

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

4. po aktualizácii obnovte pôvodný adresár `/var/cache/apt/archives`:

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

5. odstráňte zostávajúce `/media/usbkey/archives`.

Dočasný adresár vyrovnávacej pamäte balíkov môžete vytvoriť na ľubovoľnom pripojenom súborovom systéme.

- Vykonať minimálnu aktualizáciu systému (pozri Oddiel 4.4.4) alebo čiastočné aktualizácie systému nasledované úplnou aktualizáciou. To umožní aktualizovať systém po častiach a umožní vám vyčistiť vyrovnávaciu pamäť balíkov pred úplnou aktualizáciou.

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

4.4.4 Minimálna aktualizácia systému

DÔLEŽITÉ



If you are upgrading remotely, be aware of Oddiel [5.1.22](#).

V niektorých prípadoch môže priame spustenie úplnej aktualizácie odstrániť veľké množstvo balíkov, ktoré si chcete ponechať. Preto odporúčame dvojfázový proces aktualizácie. V prvej fáze minimálnu aktualizáciu, aby sa vyriešili tieto konflikty a následne úplnú aktualizáciu ako popisuje Oddiel [4.4.5](#).

Najprv spustite:

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

Toto aktualizuje tie balíky, ktoré je možné aktualizovať bez nutnosti odstránenia alebo inštalácie iných balíkov.

Minimálna aktualizácia systému tiež môže byť užitočná v prípade, keď má systém málo miesta a úplnú aktualizáciu nemožno spustiť z dôvodu obmedzeného miesta.

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 Aktualizácia systému

Po dokončení týchto krokov budete pripravený pokračovať v hlavnej časti aktualizácie. Spustite:

```
# apt full-upgrade
```

Tým sa vykoná kompletná aktualizácia systému, nainštalujú sa najnovšie dostupné verzie všetkých balíkov a vyriešia sa všetky možné zmeny závislostí medzi balíkmi v rôznych vydaniach. Ak je to potrebné, nainštalujú sa niektoré nové balíky (zvyčajne nové verzie knižníc a premenované balíky) a odstránia sa všetky konfliktné zastaralé balíky.

Pri aktualizácii z diskov CD/DVD/BD vás systém požiada o vloženie niektorých konkrétnych diskov niekoľkokrát počas aktualizácie. Je možné, že budete musieť vložiť rovnaký disk viac než raz; to je z dôvodu navzájom závisiacich balíkov, ktoré sa nachádzajú na rôznych diskoch.

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 Možné problémy počas aktualizácie

Následovné oddiely popisujú známe problémy, ktoré sa môžu vyskytnúť pri aktualizácii na bullseye.

4.5.1 Dist-upgrade zlyhá s chybou „Nebolo možné vykonať okamžitú konfiguráciu“

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 Očakávané odstránenia

Proces aktualizácie na bullseye môže požadovať odstránenie balíkov zo systému. Presný zoznam balíkov bude závisieť na množine balíkov, ktorú máte nainštalovanú. Tieto poznámky k vydaniu poskytujú všeobecné rady o metóde, ktorú by ste mali zvoliť, ale ak máte pochybnosti, odporúčame aby ste preskúmali odstránenie ktorých balíkov je navrhnuté v každej z metód. Ďalšie informácie o balíkoch, ktoré boli v bullseye označené ako zastarané nájdete v časti Oddiel 4.8.

4.5.3 Cykly Konfliktov alebo Predzávislostí

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
```

na odstránenie niektorých z konfliktných balíkov alebo

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

V extrémnych prípadoch budete musieť vynútiť reinstaláciu príkazom typu

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

4.5.4 Konflikty súborov

Konflikty súborov by sa nemali vyskytnúť ak aktualizujete z „čistého“ systému buster, ale môžu sa vyskytnúť ak máte nainštalované neoficiálne spätné porty (backports). Konflikt súborov sa prejaví nasledovnou chybou:

```
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>
```

Môžete sa pokúsiť vyriešiť konflikt súborov tým, že nasilu odstránite balík uvedený na *poslednom* riadku chybovej správy:

```
# 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 Zmeny v konfigurácii

Počas aktualizácie dostanete otázky týkajúce sa konfigurácie alebo rekonfigurácie niekoľkých balíkov. Po otázke, či nejaký súbor z adresára `/etc/init.d` alebo `/etc/manpath.config` má byť nahradený verziou od správcu balíka je zvyčajne potrebné odpovedať „áno“, aby ste zaistili konzistenciu systému. Kedykoľvek môžete vrátiť staršie verzie, pretože sa uložia s príponou `.dpkg-old`.

Ak si nie ste istý, čo máte robiť, zapíšte si meno balíka alebo súboru a veci vyriešte neskôr. Ak chcete skontrolovať informácie, ktoré boli na obrazovke počas aktualizácie, môžete hľadať v súbore záznamu relácie.

4.5.6 Zmena relácie na konzolu

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.

Na návrat na konzolu s bežiacou aktualizáciou budete musieť použiť `Ctrl + Alt + F1` (ak ste na grafickej štartovacej obrazovke) alebo `Alt + F1` (ak ste na lokálnej obrazovke v textovom režime), čo vás prepne späť na virtuálny terminál 1. Nahradte `F1` funkčným klávesom s číslom zodpovedajúcim virtuálnemu terminálu, na ktorom bežala aktualizácia. Tiež môžete použiť `Alt + šípka vľavo` alebo `Alt + šípka vpravo` na prepínanie medzi susednými terminálmi v textovom režime.

4.6 Aktualizácia jadra a súvisiacich balíkov

Táto časť vysvetľuje ako aktualizovať vaše jadro a identifikuje možné problémy týkajúce sa tejto aktualizácie. Môžete buď nainštalovať jeden z balíkov `linux-image-*`, ktoré poskytuje Debian alebo skompilovať prispôbené jadro zo zdrojových súborov.

Pamätajte, že veľa informácií v tejto časti je založených na predpoklade, že budete používať jedno z modulárnych jadier v Debiane spolu s `initramfs-tools` a `udev`. Ak sa rozhodnete použiť prispôbené jadro, ktoré nevyžaduje `initrd` alebo použijete iný nástroj na tvorbu `initrd`, niektoré z týchto informácií sa vás nemusia týkať.

4.6.1 Inštalácia metabalíka jadra

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
```

Ak nevidíte žiadny výstup, budete musieť nainštalovať nový balík `linux-image` ručne alebo nainštalovať niektorý z metabalíkov `linux-image`. Zoznam dostupných metabalíkov `linux-image` uvidíte po spustení:

```
# 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 Oddiel 5.1.24 before performing the first reboot after the upgrade.

For the more adventurous there is an easy way to compile your own custom kernel on Debian. Install the kernel sources, provided in the `linux-source` package. You can make use of the `deb-pkg` target available in the sources' makefile for building a binary package. More information can be found in the [Debian Linux Kernel Handbook](https://kernel-team.pages.debian.net/kernel-handbook/) (<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 Oddiel 4.4.4.

4.7 Príprava na ďalšie vydanie

Po aktualizácii môžete urobiť niekoľko vecí, ktorými sa pripravíte na ďalšie vydanie.

- Odstráňte nadbytočné alebo zastaralé balíky ako popisuje Oddiel 4.4.3 a Oddiel 4.8. Mali by ste skontrolovať, ktoré konfiguračné súbory používajú a zväziť vyčistenie konfigurácie balíkov (purge), aby sa odstránili ich konfiguračné súbory. Pozri aj Oddiel 4.7.1.

4.7.1 Vyčistenie (purge) odstránených balíkov

Vo všeobecnosti sa odporúča na vyčistenie odstránených balíkov. To platí najmä, ak boli balíky odstránené v predchádzajúcich aktualizáciách vydania (napr. počas aktualizácie na buster) alebo pochádzajú od tretích strán. Najmä o starých skriptoch `init.d` je známe, že spôsobujú problémy.

VÝSTRAHA



Vyčistenie balíka zvyčajne vymaže jeho súbory protokolu, preto si ich najskôr zálohujte.

Nasledovný príkaz zobrazí zoznam všetkých odstránených balíkov, ktoré mohli zanechať v systéme konfiguračné súbory (ak ich používajú):

```
# 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 }')
```

Ak používate `aptitude`, môžete použiť aj nasledovnú alternatívu k vyššie uvedeným príkazom:

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

4.8 Zastaralé balíky

Okrem toho, že bullseye prináša mnoho nových balíkov, tiež odstraňuje dosť veľa starých balíkov, ktoré obsahovalo vydanie buster. Neposkytuje pre tieto zastaralé balíky žiadnu aktualizáciu cestu. Hoci vám nič nebráni naďalej používať zastarané balíky, projekt Debian zvyčajne prestane poskytovať podporu bezpečnostných aktualizácií jeden rok po vydaní bullseye⁵ a medzitým zvyčajne neposkytuje inú podporu. Preto sa odporúča nahradiť ich alternatívami ak sú nejaké dostupné.

Existuje mnoho dôvodov, prečo môžu byť balíky z distribúcie odstránené: ich pôvodný autor ich už nespravuje; ich správa už nezaujíma vývojára Debianu; funkcionality, ktorú poskytujú nahradil iný softvér (alebo novšia verzia); alebo už sa nepovažujú za vhodné vo vydaní bullseye z dôvodu chýb. V poslednom prípade môže distribúcia „unstable“ naďalej obsahovať tieto balíky.

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

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

Systém sledovania chýb Debianu (<https://bugs.debian.org/>) často poskytne ďalšie informácie o tom, prečo bol balík odstránený. Mali by ste si prečítať archivované hlásenia chýb samotného balíka aj archivované hlásenia chýb **pseudobalíka** [ftp.debian.org](https://bugs.debian.org/cgi-bin/pkgreport.cgi?pkg=ftp.debian.org&archive=yes) (<https://bugs.debian.org/cgi-bin/pkgreport.cgi?pkg=ftp.debian.org&archive=yes>).

Zoznam zastaralých balíkov v Bullseye nájdete v Oddiel 5.3.1.

⁵Alebo ak dovedy nenaštane ďalšie vydanie. Zvyčajne sú zakaždým podporované súčasne iba dve stabilné vydania.

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.

Kapitola 5

Problémy vyskytujúce sa v bullseye

Niekedy majú zmeny zavedené v novom vydaní vedľajšie účinky, ktorým sa nedokážeme rozumne vyhnúť alebo by spôsobili objavenie chýb inde. Tu dokumentujeme problémy, ktorých sme si vedomí. Tiež si prosím prečítajte errata, dokumentáciu relevantných balíkov, hlásenia o chybách a ďalšie informácie, ktoré spomína Oddiel 6.1.

5.1 Položky týkajúce sa aktualizácie na bullseye

Táto časť pokrýva položky týkajúce sa aktualizácie z buster na bullseye

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

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

5.1.2 Changed security archive layout

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

The security line in your APT configuration may look like:

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

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

```
APT::Default-Release "/^bullseye(|-security|-updates)$/";
```

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

5.1.3 Password hashing uses yescrypt by default

The default password hash for local system accounts **has been changed** (<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`.

5.1.4 NSS NIS and NIS + support require new packages

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

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

5.1.5 Config file fragment handling in unbound

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

5.1.6 rsync parameter deprecation

The `rsync` parameter `--noatime` has been renamed `--open-noatime`. The old form is no longer supported; if you are using it you should see [the NEWS file](https://sources.debian.org/src/rsync/bullseye/debian/rsync.NEWS/) (<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/) (<https://backports.debian.org/>) repository. The version of `rsync` in the initial release of bullseye also deprecated `--copy-devices` in favor of `--write-devices`, but version `3.2.3-4+deb11u1` (included in bullseye point release 11.1) reverts this deprecation and supports both options.

5.1.7 Vim addons handling

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

5.1.8 OpenStack and cgroups v1

OpenStack Victoria (released in bullseye) requires `cgroup v1` for block device QoS. Since bullseye also changes to using `cgroupv2` by default (see [Oddiel 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.

5.1.9 OpenStack API policy files

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

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

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

5.1.10 sendmail downtime during upgrade

In contrast to normal upgrades of `sendmail`, during the upgrade of `buster` to `bullseye` the `sendmail` service will be stopped, causing more downtime than usual. For generic advice on reducing downtime see [Oddiel 4.1.3](#).

5.1.11 FUSE 3

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

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

5.1.12 GnuPG options file

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

5.1.13 Linux enables user namespaces by default

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

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

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

```
user.max_user_namespaces = 0
```

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

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

5.1.14 Linux disables unprivileged calls to bpf() by default

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

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

```
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.

5.1.15 redmine missing in bullseye

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

5.1.16 Exim 4.94

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

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

Typical nonworking examples include:

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

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

instead of

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

for a virtual domain alias file.

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

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

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

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

5.1.17 SCSI device probing is non-deterministic

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

5.1.18 rdiff-backup require lockstep upgrade of server and client

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

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

5.1.19 Intel CPU microcode issues

The `intel-microcode` package currently in bullseye and `buster-security` (see [DSA-4934-1](https://www.debian.org/security/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>) that use `firmware-iwlwifi`, and for some Skylake R0/D0 CPUs on systems using a very outdated firmware/BIOS, **the system may hang on boot** (<https://github.com/intel/Intel-Linux-Processor-Microcode-Data-Files/issues/31>).

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

5.1.20 Upgrades involving `libgc1c2` need two runs

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

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

The `fail2ban` package can be configured to send out e-mail notifications. It does that using `mail`, which is provided by multiple packages in Debian. A security update (needed on systems that use `mail` from `mailutils`) just before the release of bullseye broke this functionality for systems that have `mail` provided by `bsd-mailx`. Users of `fail2ban` in combination with `bsd-mailx` who wish `fail2ban` to send out e-mail should either switch to a different provider for `mail` or manually unapply [the upstream commit](https://github.com/fail2ban/fail2ban/commit/410a6ce5c80dd981c22752da034f2529b5eee8) (<https://github.com/fail2ban/fail2ban/commit/410a6ce5c80dd981c22752da034f2529b5eee8>) (which inserted the string `"-E 'set escape'"` in multiple places under `/etc/fail2ban/action.d/`).

5.1.22 No new SSH connections possible during upgrade

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

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

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

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

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

5.1.24 Čo urobiť po aktualizácii pred reštartom

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 Obmedzenia bezpečnostnej podpory

Existujú niektoré balíky, pre ktoré Debian nemôže sľúbiť poskytovanie minimálnych spätných portov v prípade bezpečnostných problémov. Tieto sú popísané v nasledovných častiach.

POZNÁMKA



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 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>).

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

5.2.4 32-bit Xen PV guests are not supported

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

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

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

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

5.3 Obsolescence and deprecation

5.3.1 Významné zastaralé balíky

Nasleduje zoznam známych významných zastaralých balíkov (ich popis nájdete v Oddiel 4.8).

Medzi zastaralé balíky patria:

- The `lilo` package has been removed from bullseye. The successor of lilo as boot loader is `grub2`.
- The Mailman mailing list manager suite version 3 is the only available version of Mailman in this release. Mailman has been split up into various components; the core is available in the package `mailman3` and the full suite can be obtained via the `mailman3-full` metapackage.
The legacy Mailman version 2.1 is no longer available (this used to be the package `mailman`). This branch depends on Python 2 which is no longer available in Debian.
For upgrading instructions, please see [the project's migration documentation](https://docs.mailman3.org/en/latest/migration.html). (<https://docs.mailman3.org/en/latest/migration.html>)
- The Linux kernel no longer provides `isdn4linux (i4l)` support. Consequently, the related user-land packages `isdnutils`, `isdnactivecards`, `drdsl` and `ibod` have been removed from the archives.
- The deprecated `libappindicator` libraries are no longer provided. As a result, the related packages `libappindicator1`, `libappindicator3-1` and `libappindicator-dev` are no longer available. This is expected to cause dependency errors for third-party software that still depends on `libappindicator` to provide system tray and indicator support.
Debian is using `libayatana-appindicator` as the successor of `libappindicator`. For technical background see [this announcement](https://lists.debian.org/debian-devel/2018/03/msg00506.html) (<https://lists.debian.org/debian-devel/2018/03/msg00506.html>).
- Debian no longer provides `chef`. If you use Chef for configuration management, the best upgrade path is probably to switch to using the packages provided by [Chef Inc](https://www.chef.io/) (<https://www.chef.io/>).
For background on the removal, see [the removal request](https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=963750) (<https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=963750>).
- Python 2 is already beyond its End Of Life, and will receive no security updates. It is not supported for running applications, and packages relying on it have either been switched to Python 3 or removed. However, Debian bullseye does still include a version of Python 2.7, as well as a small number of Python 2 build tools such as `python-setuptools`. These are present only because they are required for a few application build processes that have not yet been converted to Python 3.
- The `aufs-dkms` package is not part of bullseye. Most `aufs-dkms` users should be able to switch to `overlayfs`, which provides similar functionality with kernel support. However, it's possible to have a Debian installation on a filesystem that is not compatible with `overlayfs`, e.g. `xf`s 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 Zastaralé súčasti bullseye

S ďalším vydaním Debian 12 (s kódovým označením bookworm) niektoré funkcie budú označené ako zastarané. Používatelia budú musieť migrovať na iné alternatívy, aby predišli problémom pri aktualizácii na Debian 12.

Medzi ne patria nasledovné funkcie:

- 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)	<code>ca-certificates-java</code>	<code>ca-certificates-java: /etc/ca-certificates/update.d/jks-keystore doesn't update /etc/ssl/certs/java/cacerts</code>
990026 (https://bugs.debian.org/990026)	<code>cron</code>	<code>cron: Reduced charset in MAILTO causes breakage</code>
991081 (https://bugs.debian.org/991081)	<code>gir1.2-diodon-1.0</code>	<code>gir1.2-diodon-1.0 lacks dependencies</code>
990318 (https://bugs.debian.org/990318)	<code>python-pkg-resources</code>	<code>python-pkg-resources: please add Breaks against the unversioned python packages</code>
991449 (https://bugs.debian.org/991449)	<code>fail2ban</code>	<code>fix for CVE-2021-32749 breaks systems with mail from bsd-mailx</code>

Bug number	Package (source or binary)	Description
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/emacs-common/packages/install/git emacs failed at /usr/lib/emacs-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)	gparsed	gparsed should not mask .mount units
984714 (https://bugs.debian.org/984714)	gparsed	gparsed should suggest exfatprogs and backport the commit that rejects exfat-utils
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
982459 (https://bugs.debian.org/982459)	mdadm	mdadm --examine in chroot without /proc,/dev,/sys mounted corrupts host's file-system
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

Bug number	Package (source or binary)	Description
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.map -> ../../../../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

Kapitola 6

Ďalšie informácie o Debiane

6.1 Ďalšie čítanie

Okrem týchto Poznámok k vydaniu a Inštaláčnej príručky ďalšiu dokumentáciu o systéme Debian nájdete v rámci Dokumentačného projektu Debian (DDP), ktorého cieľom je tvoriť kvalitnú dokumentáciu pre používateľov a vývojárov Debianu. Medzi dostupnú dokumentáciu patrí Debian Reference, Debian New Maintainers Guide, Debian FAQ a mnohé ďalšie. Podrobnosti o existujúcich zdrojoch nájdete na [webstránke DDP](https://www.debian.org/doc/) (<https://www.debian.org/doc/>) a na [Debian Wiki](https://wiki.debian.org/) (<https://wiki.debian.org/>).

Dokumentácia jednotlivých balíkov sa inštaluje do adresára `/usr/share/doc/balík`. Sem patria informácie o autorských právach, podrobnosti o balíku špecifické pre Debian a všetka dokumentácia pochádzajúca od pôvodných autorov.

6.2 Ako získať pomoc

Existuje mnoho spôsobov ako získať pomoc, rady a podporu pri používaní Debianu, no mali by ste ich zvážiť až potom, čo ste pri skúmaní problému prehľadali všetku dostupnú dokumentáciu. Tento oddiel poskytuje krátky úvod k tým informačným kanálom, ktoré môžu pomôcť novým používateľom Debianu.

6.2.1 Konferencie

Konferencie elektronickej pošty, ktoré najviac zaujímajú používateľov Debianu, sú `debian-user` (po anglicky) a ostatné konferencie `debian-user-jazyk` (v ostatných jazykoch). Informácie o týchto konferenciách a ako sa do nich prihlásiť popisuje <https://lists.debian.org/>. Rešpektujte prosím štandardnú etiketu elektronickej komunikácie a konferencií a než pošlete svoju otázku, pohľadajte najskôr v archívoch konferencie či sa ju už niekto pýtal.

6.2.2 Internet Relay Chat

Debian má na IRC sieti OFTC kanál určený na podporu a pomoc používateľom Debianu. Kanál nájdete pod menom `#debian` na serveri `irc.debian.org`.

Prosím, dodržiavajte pravidlá kanála a berte ohľad na ostatných používateľov. Pravidlá nájdete na [Debian Wiki](https://wiki.debian.org/DebianIRC) (<https://wiki.debian.org/DebianIRC>).

Ďalšie informácie o OFTC nájdete na jeho [webovej stránke](http://www.oftc.net/) (<http://www.oftc.net/>).

6.3 Oznamovanie chýb

Snažíme sa, aby sme z Debianu urobili kvalitný operačný systém - to však neznamená, že balíky, ktoré poskytujeme nemajú vôbec žiadne chyby. V súlade s filozofiou “otvoreného vývoja” Debianu a ako službu našim používateľom sprístupňujeme všetky informácie o nahlásených chybách v našom vlastnom Systéme sledovania chýb (BTS). BTS je možné prehliadať na adrese <https://bugs.debian.org/>.

Ak nájdete chybu v distribúcii alebo v niektorom z balíkov softvéru, ktorý je jej súčasťou, oznámte ju prosím, aby ju bolo možné riadne opraviť v ďalších vydaniach. Na oznámenie chyby je potrebné

mať platnú emailovú adresu. Vyžadujeme ju preto, aby sme mohli sledovať chyby a aby mohli vývojári kontaktovať oznamovateľov, ak potrebujú podrobnejšie informácie.

Hlásenie o chybe môžete poslať pomocou programu **reportbug** alebo manuálne zaslaním emailu. Viac o Systéme sledovania chýb a ako ho používať sa dozviete v jeho dokumentácii (v `/usr/share/doc/debian` ak máte nainštalovaný balík `doc-debian`) alebo online na stránke **Systému sledovania chýb** (<https://bugs.debian.org/>).

6.4 Ako prispievať do Debianu

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.

Ak chcete venovať viac času, môžete v rámci Debianu spravovať časť kolekcie slobodného softvéru. Obzvlášť užitočné je, ak ľudia prevezmú alebo začnú spravovať veci, ktoré si niekto vyžiadal zaradiť do Debianu. Podrobnosti o tomto nájdete v **databáze balíkov, ktoré potrebujú pomoc a perspektívnych balíkov** (<https://www.debian.org/devel/wnpp/>). Ak vás zaujímajú konkrétne skupiny, môže vás baviť účasť v niektorom z podprojektov Debianu, kam patria okrem iného porty na rôzne architektúry a **Debian Pure Blends** (<https://wiki.debian.org/DebianPureBlends>) pre špecifické skupiny používateľov.

V každom prípade, ak sa akýmkoľvek spôsobom podieľate na komunite slobodného softvéru, či ako používateľ, programátor, tvorca dokumentácie alebo prekladateľ, pomáhate tým hnutiu slobodného softvéru. Prispievanie je veľmi užitočné a často aj zábavné, umožňuje vám spoznať nových ľudí a dáva vám ťažko popísateľný hrejivý pocit.

Kapitola 7

Slovník

ACPI

Advanced Configuration and Power Interface (pokročilé rozhranie na správu konfigurácie a napájania)

ALSA

Advanced Linux Sound Architecture (pokročilá zvuková architektúra Linuxu)

BD

Blu-ray Disc (disk Blu-ray)

CD

Compact Disc (disk CD)

CD-ROM

Compact Disc Read Only Memory (disk CD-ROM, len na čítanie)

DHCP

Dynamic Host Configuration Protocol (protokol na dynamickú konfiguráciu počítačov)

DLBD

Dual Layer Blu-ray Disc (dvojvrstvový disk Blu-ray)

DNS

Domain Name System (systém názvov domén)

DVD

Digital Versatile Disc (disk DVD)

GIMP

GNU Image Manipulation Program (program GNU na prácu s obrázkami)

GNU

GNU's Not Unix (GNU nie je Unix)

GPG

GNU Privacy Guard (program GNU na ochranu súkromia)

LDAP

Lightweight Directory Access Protocol (nenáročný protokol na prístup k adresárom)

LSB

Linux Standard Base (štandardný základ Linuxu)

LVM

Logical Volume Manager (správca logických zväzkov)

MTA

Mail Transport Agent (agent na prenos pošty)

NBD

Network Block Device (sieťové blokové zariadenie)

NFS

Network File System (sieťový súborový systém)

NIC

Network Interface Card (karta sieťového rozhrania)

NIS

Network Information Service (sieťová informačná služba)

PHP

PHP: Hypertext Preprocessor (PHP - preprocesor hypertextu)

RAID

Redundant Array of Independent Disks (redundantné (nadbytočné) pole nezávislých diskov)

SATA

Serial Advanced Technology Attachment

SSL

Secure Sockets Layer (zabezpečená vrstva socketov)

TLS

Transport Layer Security (zabezpečenie transportnej vrstvy)

UEFI

Unified Extensible Firmware Interface (zjednotené rozšíriteľné firmvérové rozhranie)

USB

Universal Serial Bus (univerzálna sériové zbernica)

UUID

Universally Unique Identifier (univerzálny jedinečný identifikátor)

WPA

Wi-Fi Protected Access (chránený prístup k Wi-Fi)

Dodatok A

Ako spravovať váš systém buster pred aktualizáciou

Táto príloha obsahuje informácie o tom, ako sa môžete uistiť, že dokážete inštalovať a aktualizovať balíky buster pred aktualizáciou na bullseye. Malo by to byť potrebné iba v určitých situáciách.

A.1 Ako aktualizovať váš systém buster

V podstate sa to nelíši od bežnej aktualizácie buster, akú ste vykonávali doteraz. Jediný rozdiel je v tom, že sa musíte uistiť, že váš zoznam balíkov ešte stále obsahuje odkazy na buster, ako vysvetľuje Oddiel [A.2](#).

Ak aktualizujete svoj systém pomocou zrkadla Debianu, bude automaticky aktualizovaný na najnovšiu aktualizáciu stabilnej vetvy (point release) buster.

A.2 Checking your APT source-list files

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

Ak ste už navyše nainštalovali balíky z bullseye, už pravdepodobne nemá zmysel inštalovať balíky z buster. V tom prípade sa budete musieť sami rozhodnúť či chcete pokračovať alebo nie. Je možné znížiť verziu balíkov, ale to tento dokument nepopisuje.

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.

DÔLEŽITÉ



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.

Ak ste vykonali nejaké zmeny, uložte súbor a spustite

```
# apt update
```

aby sa aktualizoval zoznam balíkov.

A.3 Odstránenie zastaralých konfiguračných súborov

Pred aktualizáciou systému na bullseye sa odporúča odstrániť zo systému staré konfiguračné súbory (napríklad súbory *.dpkg-{new,old} súbory v /etc).

Dodatok B

Prispievatelia do Poznámok k vydaniu

Vzniku týchto Poznámok k vydaniu pomohli mnohí ľudia, okrem iných aj

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

Tento dokument bol preložený do mnohých jazykov. Vďaka prekladateľom!

Do slovenčiny preložil: Ivan Masár.

Register

A

Apache, 4

B

BIND, 4

C

Calligra, 3

Cryptsetup, 4

D

DocBook XML, 2

Dovecot, 4

E

Exim, 4

G

GCC, 4

GIMP, 4

GNOME, 3

GNUCash, 3

GnuPG, 4

I

Inkscape, 4

K

KDE, 3

L

LibreOffice, 3

LXDE, 3

LXQt, 3

M

MariaDB, 4

MATE, 3

N

Nginx, 4

O

OpenJDK, 4

OpenSSH, 4

P

packages

apt, 1, 2, 14, 25

apt-listchanges, 18

aptitude, 12, 17, 21

aufs-dkms, 29

bazel-bootstrap, 6

bsd-mailx, 27

ca-certificates-java, 30

chef, 29

cinder-volume, 24

connman, 29

cron, 30

cups-browsed, 4

cups-daemon, 4

cups-filters, 4

dblatex, 2

debian-goodies, 17

debian-kernel-handbook, 20

debian-security-support, 27

doc-debian, 34

docbook-xsl, 2

dpkg, 1

drdsl, 29

exfat-fuse, 5

exfat-utils, 6

exfatprogs, 6

fail2ban, 27, 30

firmware-iwlwifi, 26

fuse, 25

fuse3, 25

gcc-10-base, 31

gir1.2-diodon-1.0, 30

gir1.2-gtd-1.0, 31

git-el, 31

glibc, 24

gnome-control-center, 28

gparted, 31

grub2, 29

guile-2.2-libs, 27

gvfs-fuse, 25

how-can-i-help, 34

ibod, 29

ifenslave, 31

initramfs-tools, 10, 20

intel-microcode, 26, 27

ipp-usb, 4, 5

isdnactivecards, 29

isdnutils, 29

kio-fuse, 25

libappindicator-dev, 29

libappindicator1, 29

libappindicator3-1, 29

libayatana-appindicator, 29

libgc1c2, 27

libjs-bootstrap4, 32

libnss-nis, 24

libnss-nisplus, 24

libpam-chroot, 31

libpython3.9-dev, 31

libsane1, 4, 5

lilo, 29

linux-image-*, 20

linux-image-amd64, 20

linux-source, 20

localepurge, 17

mailman, 29

mailman3, 29

mailman3-full, 29
mailutils, 27
mariadb-server-10.5.galera-4, 31
mdadm, 31
network-manager, 29
nova-compute, 24
openipmi, 31
openssh-server, 27, 31
openvswitch, 27
popularity-contest, 17
procps, 31
pulseaudio, 31
python-pkg-resources, 30
python-setuptools, 29
rails, 25
rdiff-backup, 26
redmine, 25
release-notes, 1
rsync, 24
rsyslog, 5
sane-airscan, 4
sendmail, 25
slapd, 30
speech-dispatcher, 32
src:gcc-10, 31
src:llvm-toolchain-11, 31
src:qemu, 32
src:squid-deb-proxy, 32
src:wine, 32
src:xen, 32
sshfs, 25
synaptic, 12
systemd, 6
tinc, 11
tpm2-abrmd, 32
udev, 20, 26
unbound, 24
upgrade-reports, 1
usrmerge, 30
vim, 24
vim-addon-manager, 24
vim-scripts, 24
wicd, 29
xen, 29
xfce4-settings, 32
xmlroff, 2
xsltproc, 2

Perl, 4
PHP, 4
Postfix, 4
PostgreSQL, 4

X
Xfce, 3