Udgivelsesnoter til Debian 11 (bullseye), 32-bit PC

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

26. juni 2022

Indhold

Kapitel 1

Introduktion

Dette dokument informerer brugere af Debian-distributionen om større ændringer i version 11 (kodenavn bullseye).

Udgivelsesnoterne har information om, hvordan du sikkert opgraderer fra version 10 (kodenavn buster) til den aktuelle udgave og informerer brugere om kendte problemstillinger, som kan opstå under opgraderingen.

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

PAS PÅ

Bemærk at det er umuligt at skrive om alle kendte problemstillinger, og at udvælgelsen er baseret på en kombination af forventet forekomst og omfang.

Bemærk at vi alene understøtter og dokumenterer opgradering fra den forrige version af Debian (i dette tilfælde, opgradering fra buster). Hvis du har brug for at opgradere fra en ældre version, foreslår vi, at du læser tidligere udgaver af udgivelsesnoterne og først opgraderer til buster.

1.1 Rapporter fejl i dette dokument

Vi har forsøgt at teste alle trin i opgraderingen, som beskrives i det her dokument og at forudse alle de mulige problemstillinger, som en bruger kan møde.

Nevertheless, if you think you have found a bug (incorrect information or information that is missing) in this documentation, please file a bug in the bug tracking system (https://bugs.debian.org/) against the release-notes package. You might first want to review the existing bug reports (https://bugs.debian.org/release-notes) in case the issue you've found has already been reported. Feel free to add additional information to existing bug reports if you can contribute content for this document.

Vi er taknemlige for og opfordrer til fejlrettelser til dokumentets kilder, som er vedhæftet fejlrapporten. Du kan finde yderligere information, der beskriver hvordan du kan finde kilderne til dette dokument, i Afsnit 1.3.

1.2 Bidrag med opgraderingsrapporter

Vi er glade for al information fra brugere, som har forbindelse til opgraderinger fra buster til bullseye. Hvis du vil dele din information med os, så kan du sende denne ind via en fejlrapport i fejlrapporteringssystemet (https://bugs.debian.org/) mod pakken upgrade-reports med dine erfaringer. Vi vil bede dig om, at du komprimerer eventuelle bilag som inkluderes (med **gzip**).

Inkluder følgende information når du indsender din opgraderingsrapport:

- Status på din pakkedatabase før og efter opgraderingen: `dpkg`'s statusdatabase tilgængelig i `/var/lib/dpkg/status` og `apt`'s pakketilstandsinformation, tilgængelig i `/var/lib/apt/extended_states`. Du bør lave en sikkerhedskopi før opgraderingen som beskrevet i Afsnit 4.1.1, men du kan også finde sikkerhedskopier af `/var/lib/dpkg/status` i `/var/backups`.
- Sessionslog fra **script**, læs mere om dette i Afsnit 4.4.1.
- Dine `apt`-logge, tilgængelige i `/var/log/apt/term.log` eller dine **aptitude**-logge tilgængelige i `/var/log/aptitude`.

BEMÆRK

Du bør gennemgå og fjerne al personlig og/eller fortrolig information fra logge, før du inkluderer dem i en fejlrapport, da informationen vil blive udgivet i en offentlig database.

1.3 Kilder til dette dokument

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`).

Kapitel 2

Nyt i Debian 11

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

2.1 Understøttede arkitekturer

Følgende er de officielt understøttede arkitekturer i Debian 11:

- 32-bit pc (i386) og 64-bit pc (amd64)
- 64-bit ARM (arm64)
- ARM EABI (armel)
- ARMv7 (EABI hard-float ABI, armhf)
- little-endian MIPS (mipsel)
- 64-bit little-endian MIPS (mips64el)
- 64-bit little-endian PowerPC (ppc64el)
- IBM System z (s390x)

Du kan læse mere om porteringsstatus og porteringsspecifik information om din arkitektur på Debians websider om porteringer (https://www.debian.org/ports/).

2.2 Nyt i distributionen

Denne nye udgave af Debian leveres med mange flere programmer end dens forgænger buster. Distributionen indeholder over 11294 nye pakker, og i alt 59551 pakker. De fleste programmer i distributionen er blevet opdateret: over 42821 softwarepakker (dette svarer til 72 % af alle pakker i buster). Et betydeligt antal pakker (over 9519, 16 % af alle pakker i buster) er af forskellige grunde blevet fjernet fra distributionen. Du vil ikke se opdateringer for disse pakker, og de markeres »forældet« i pakkehåndteringsprogrammer; se Afsnit 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.

Produktivitetsprogrammer er også blevet opgraderet, inklusive kontorpakkerne:

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

Blandt meget andet inkluderer denne udgave følgende opdateringer:

Pakker	Version i 10 (buster)	Version i 11 (bullseye)
Apache	2.4.38	2.4.48
BIND DNS-server	9.11	9.16
Cryptsetup	2.1	2.3
Dovecot MTA	2.3.4	2.3.13
Emacs	26.1	27.1
Exim som standard-e-postserver	4.92	4.94
GNU Compiler Collection som standardcompiler	8.3	10.2
GIMP	2.10.8	2.10.22
GnuPG	2.2.12	2.2.27
Inkscape	0.92.4	1.0.2
GNU C-programbiblioteket	2.28	2.31
lighttpd	1.4.53	1.4.59
Linux-kerneaftryk	4.19 series	5.10 series
LLVM/Clang toolchain	6.0.1 and 7.0.1 (default)	9.0.1 and 11.0.1 (default)
MariaDB	10.3	10.5
Nginx	1.14	1.18
OpenJDK	11	11
OpenSSH	7.9p1	8.4p1
Perl	5.28	5.32
PHP	7.3	7.4
Postfix MTA	3.4	3.5
PostgreSQL	11	13
Python 3	3.7.3	3.9.1
Rustc	1.41 (1.34 for `armel`)	1.48
Samba	4.9	4.13
Vim	8.1	8.2

2.2.2 Driverless scanning and printing

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

2.2.2.1 CUPS and driverless printing

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

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

2.2.2.2 SANE and driverless scanning

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

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

2.2.3 New generic open command

A new **open** command is available as a convenience alias to **xdg-open** (by default) or **run-mailcap**, managed by the update-alternatives(1) (https://manpages.debian.org//bullseye/dpkg/update-alternati 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 Afsnit 5.1.9 section.

2.2.5 Persistent systemd journal

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

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

2.2.6 New Fcitx 5 Input Method

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

2.2.7 News from 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) 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`).

Kapitel 3

Installeringssystemet

Debian Installer er Debians officielle installeringssystem. Det tilbyder en række forskellige installeringsmetoder. Hvilke af disse som fungerer på dit system, afhænger af din platform.

Aftryk af installeringsprogrammet til bullseye kan findes sammen med installeringsguiden på Debians hjemmeside (`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/da/index.html
```

Du vil måske også læse errata (`https://www.debian.org/releases/bullseye/debian-installer/index#errata`) til debian-installer hvor en liste over kendte problemer findes.

3.1 Hvad er nyt i installeringssystemet?

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

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

3.1.1 Help with installation of firmware

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

This new functionality is restricted to the unofficial installer images with firmware included (see https://www.debian.org/releases/bullseye/debian-installer/#firmware_nonfree (`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-instal`

3.1.2 Automatisk installering

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.

Installeringsguiden (`https://www.debian.org/releases/bullseye/installmanual`) har et separat bilag med omfattende dokumentation for, hvordan forindstillinger skal bruges.

3.2 Container and Virtual Machine images

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

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

Kapitel 4

Opgraderinger fra Debian 10 (buster)

4.1 Forberedelse af opgraderingen

Du bør læse informationen i Kapitel 5, inden du opgraderer. Det kapitel dækker mulige problemer, som ikke er direkte relateret til opgraderingsprocessen, men som stadig kan være vigtige at kende til, inden du begynder.

4.1.1 Sikkerhedskopier alle data og konfigurationsinformation

Inden opgradering af dit system anbefales det kraftigt, at du foretager en fuldstændig sikkerhedskopiering, eller i det mindste laver en sikkerhedskopi af alle de data og den konfigurationsinformation, som du ikke vil risikere at miste. Opgraderingsværktøjerne og -processen er meget pålidelige, men en maskinel fejl midt i en opgradering kan resultere i et alvorligt skadet system.

De vigtigste dele, det vil være en god ide at lave sikkerhedskopier af, er indholdet af `/etc`, `/var/lib/dpkg`, `/var/lib/apt/extended_states` og uddata fra `dpkg --get-selections "*"` (citationstegn er vigtige). Hvis du bruger **aptitude** til at hente pakker på dit system, vil en sikkerhedskopiering af `/var/lib/aptitude/pkgstates` også være en god ide.

Selve opgraderingsprocessen ændrer ingenting i mappen `/home`. Dog er det kendt at visse programmer (for eksempel dele af Mozilla-pakken og skrivebordsmiljøerne GNOME og KDE) overskriver eksisterende brugerindstillinger med nye standardværdier, når en ny version af programmet startes for første gang af en bruger. Som en sikkerhedsforanstaltning bør du foretage en sikkerhedskopiering af de skjulte filer og mapper (såkaldte "punktum-filer") i brugernes hjemmemapper. Denne sikkerhedskopiering kan hjælpe til at gendanne eller genoprette de gamle indstillinger. Du ønsker måske også at informere dine brugere om dette.

Alle pakkeinstallationshandlinger skal køres med superbrugerprivilegier, så log ind som `root` (administrator) eller brug **su** eller **sudo** for at få de nødvendige adgangsrettigheder.

Opgraderingen har nogle få forudsætninger; du bør tjekke dem, før du gennemfører opgraderingen.

4.1.2 Informer brugerne i forvejen

Det er klogt at informere alle brugerne i forvejen om eventuelle opgraderinger, du planlægger, også selv om brugere der tilgår dit system via en **ssh**-forbindelse ikke vil mærke meget under opgraderingen, og bør kunne fortsætte deres arbejde.

Hvis du vil være ekstra omhyggelig, så lav en sikkerhedskopi af eller afmonter `/home` før opgraderingen.

Du skal udføre en kerneopgradering under opgraderingen til bullseye, så en genstart er nødvendig. Typisk vil dette udføres efter opgraderingen er afsluttet.

4.1.3 Forbered nedetid for tjenester

Under opgraderingsprocessen kan der være tjenester, som er tilknyttet pakker, som er en del af opgraderingen. Hvis dette er tilfældet, vil disse tjenester måske stoppe mens pakkerne, som skal opgraderes bliver omplaceret og konfigureret. I dette tidsrum vil disse tjenester ikke være tilgængelige.

Præcis hvor lang nedetiden er for disse tjenester vil afhænge af antallet af pakker, som opgraderes på systemet, og vil også inkludere den tid som systemadministratoren er om at besvare konfigurationsspørgsmål fra forskellige pakkeopgraderinger. Bemærk at hvis opgraderingsprocessen foregår uovervåget og systemet kræver svar under opgraderingen, er der stor sandsynlighed for, at tjenester er utilgængelige[1] i en væsentlig tidsperiode.

Hvis systemet som opgraderes tilbyder kritiske tjenester for dine brugere eller netværk[2], så kan du minimere nedetiden, hvis du foretager en minimal systemopgradering som beskrevet i Afsnit 4.4.4, efterfulgt af en kerneopgradering og en genstart og efterfølgende opgraderer pakker, som hører til dine kritiske tjenester. Opgrader disse pakker inden den komplette opgradering udføres jævnfør instruktionen i Afsnit 4.4.5. På denne måde kan du sikre dig, at disse vigtige tjenester er startet op og er tilgængelige gennem hele opgraderingsprocessen, og at deres nedetid er reduceret.

4.1.4 Forbered for gendannelse

Selom Debian forsøger at sikre, a dit system kan startes op på alle tidspunkter, er der en reel risko for, at du kan opleve problemer efter genstart af dit system, når opgraderingen er færdig. En del kendte problemer er dokumenteret i dette og de næste kapitler af udgivelsesnoterne.

Af den grund er det klogt at sikre sig, at du vil kunne gendanne dit system, såfremt det skulle fejle i at genstarte eller, for eksternt håndterede systemer, ikke kan få netværket til at fungere.

Hvis du fjernopgraderer via en **ssh**-henvisning, anbefales det kraftigt, at du foretager de nødvendige forholdsregler for at kunne tilgå serveren via en ekstern seriel terminal. Der er en risiko for, at efter opgradering af kernen og en genstart, at du skal rette systemkonfigurationen via en lokal konsol. Hvis systemet ved et uheld genstartes i midten af en opgradering, er der en risiko for, at du vil skulle gendanne via en lokal konsol.

For emergency recovery we generally recommend using the *rescue mode* of the bullseye Debian Installer. The advantage of using the installer is that you can choose between its many methods to find one that best suits your situation. For more information, please consult the section “Recovering a Broken System” in chapter 8 of the Installation Guide (`https://www.debian.org/releases/bullseye/installmanual`) and the Debian Installer FAQ (`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 Fejlsøg skal under opstart med initrd

Pakken `initramfs-tools` inkluderer en fejlsøgningsskal[3] i initrds’en den opretter. Hvis for eksempel initrd’en ikke kan montere dit rodfilsystem, vil du blive placeret i denne fejlsøgningsskal, som har nogle grundlæggende kommandoer tilgængelige til at hjælpe med at spore problemet og eventuelt rette det.

Grundlæggende ting der kan kontrolleres: tilstedeværelse af korrekte enhedsfiler i `/dev`; hvilke moduler indlæses (`cat /proc/modules`); resultat af **dmesg** for fejl under indlæsning af drivere. Resultatet af **dmesg** vil også vise hvilke enhedsfiler, der er blevet tildelt til hvilke diske; du bør kontrollere det imod resultatet af `echo $ROOT` for at sikre, at rodfilsystemet er på den forventede enhed.

Hvis du lykkes med at rette problemet, vil indtastning af `exit` afslutte fejlsøgningsskallen og fortsætte opstartsprocessen på det punkt hvor den fejlede. Selvfølgelig skal du også rette det underliggende problem og genoprette initrd’en så den næste opstart ikke fejler igen.

4.1.4.2 Fejlsøg skal under opstart med systemd

Hvis opstarten fejler under systemd, er det muligt at indhente en fejlsøg root-skal ved at ændre kernens kommandolinje. Hvis standardopstarten lykkes, men nogle tjenester ikke kan starte, så kan det være nyttigt at tilføje `systemd.unit=rescue.target` til kerneparametrene.

[1] Hvis debconf-prioriteten er sat til et meget højt niveau kan du måske forhindre konfigurationsprompter, men tjenester som afhænger af standardsvar som ikke er gældende for dit system vil ikke starte.

[2] Eksempelvis: DNS- eller DHCP-tjenester, specielt hvis der ikke er nogen redundans eller reserve. I tilfældet med DHCP kan slutbrugere blive frakoblet fra netværket, hvis låneperioden er kortere end tiden, det tager for opgraderingsprocessen at blive færdig.

[3] Denne funktion kan deaktiveres ved at tilføje parameteren `panic=0` til dine opstartsparametre.

Ellers vil kerneparameteren `systemd.unit=emergency.target` tilbyde dig en root-skal på det tidligste mulige punkt. Dette gøres dog før montering af root-filsystemet med læse-skrive rettigheder. Du skal gøre det manuelt med:

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

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

4.1.5 Forbered et sikkert miljø for opgraderingen

VIGTIGT

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

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

4.2 Start from “pure” Debian

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

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

4.2.1 Upgrade to Debian 10 (buster)

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

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

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

4.2.2 Remove non-Debian packages

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

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

4.2.3 Upgrade to latest point release

This procedure assumes your system has been updated to the latest point release of buster. If you have not done this or are unsure, follow the instructions in Afsnit 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 Afsnit 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 Afsnit 5.1.3.

4.2.8 Afsnittet foreslåede opdateringer (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 Uofficielle kilder

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.

Nogle brugere kan have *uofficielle* tilbageporterede "nyere" versioner af pakker som i Debian *er* installeret på deres buster-system. Sådanne pakker vil højst sandsynlig medføre problemer under en opgradering, da de kan resultere i filkonflikter[4]. Afsnit 4.5 har lidt information om hvordan filkonflikter skal håndteres, såfremt de opstår.

4.2.10 Deaktivering af 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] Debians pakkehåndteringssystem tillader normalt ikke at en pakke fjerner en fil ejet af en anden pakke medmindre, at den er blevet defineret til at erstatte denne pakke.

4.2.11 Check package status

Uanset den anvendte opgraderingsmetode, så anbefales det, at du kontrollerer pakkernes status først, og verificerer at alle pakker er i en opgraderbar tilstand. Den følgende kommando vil vise alle pakker, som har en status som halvt installeret (Half-Installed) eller som ikke kunne konfigureres, (Failed-Config) og dem med en eventuel fejlstatus.

```
# dpkg --audit
```

Du kan også inspicere tilstanden for alle pakker på dit system med **aptitude**, eller med kommandoer såsom

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

eller

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

Det er ønskværdigt at fjerne alle pakker på hold før en opgradering. Hvis en pakke - som er essentiel for opgraderingen - er på hold, så vil opgraderingen fejle.

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$'
```

Hvis du ændrede og genkompilerede en pakke lokalt, og ikke omdøbte den eller placerede en epoch i versionen, så skal du sætte den på hold for at forhindre at den bliver opgraderet.

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

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

Erstat `hold` med `install` for at fjerne tilstanden "hold".

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 Afsnit 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.

En udgivelse kan ofte refereres til både efter dets kodenavn (f.eks. `buster`, `bullseye`) og efter sit statusnavn (dvs. `oldstable`, `stable`, `testing`, `unstable`). En reference til en udgivelse med sit kodenavn har den fordel, at du aldrig vil blive overrasket af en ny udgivelse og er derfor fremgangsmåden anvendt her. Det betyder selvfølgelig, at du selv skal holde øje med udgivelsesnoter. Hvis du bruger statusnavnet i stedet for, så vil du bare se en masse opdateringer for pakker så snart en udgivelse er tilgængelig.

Debian provides two announcement mailing lists to help you stay up to date on relevant information related to Debian releases:

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

4.3.1 Tilføjelse af APT-internetkilder

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).

For example, suppose your closest Debian mirror is http://mirrors.kernel.org. If you inspect that mirror with a web browser, you will notice that the main directories are organized like this:

```
http://mirrors.kernel.org/debian/dists/bullseye/main/binary-i386/...
http://mirrors.kernel.org/debian/dists/bullseye/contrib/binary-i386/...
```

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
```

Bemærk at "dists" tilføjes implicit, og parametrene efter udgivelsesnavnet bruges til at udvide stien til flere mapper.

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

4.3.2 Tilføjelse af APT-kilder for et lokalt spejl

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).

For example, your package mirror may be under /var/local/debian/, and have main directories like this:

```
/var/local/debian/dists/bullseye/main/binary-i386/...
/var/local/debian/dists/bullseye/contrib/binary-i386/...
```

For at bruge dette med apt, så tilføj denne linje til din sources.list-fil:

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

Bemærk at "dists" tilføjes implicit, og parametrene efter udgivelsesnavnet bruges til at udvide stien til flere mapper.

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 Tilføjelse af APT-kilder fra et optisk medie

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.

Sikr dig, at der er en linje i `/etc/fstab` som aktiverer montering af dit cd-rom-drev på monteringspunktet `/media/cdrom`. For eksempel hvis `/dev/sr0` er dit cd-rom-drev, så skal `/etc/fstab` indeholde en linje som vist her:

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

Bemærk at der ikke må være *mellemrum* mellem ordene `noauto,ro` i det fjerde felt.

For at verificere, at det virker, så indsæt en cd og prøv igen

```
# 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
```

Næste, kør:

```
# apt-cdrom add
```

for hver Debian binær cd-rom du har, at tilføje dataene om hver cd til APT's database.

4.4 Opgradering af pakker

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

BEMÆRK

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.

Glem ikke at montere alle krævede partitioner (vigtigst partitionerne for root og `/usr` som skrivbare med en kommando såsom:

```
# 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.

BEMÆRK

Kildelinjer for en cd-rom kan undertiden referere til "`unstable`"; selvom dette kan være forvirrende, så skal du *ikke* ændre det.

4.4.1 Optagelse af sessionen

Det anbefales at du bruger programmet **/usr/bin/script** til at optage et sammendrag af opgraderingssessionen. Hvis der så opstår et problem, så vil du have en log over hvad der skete, og hvis krævet, kan give præcis information i en fejlrapport. For at starte registreringen tastes:

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

eller lignende. Hvis du skal køre typeskriptet igen (f.eks. hvis du skal genstarte systemet) så brug forskellige værdier for *step* for at indikere hvilket trin af opgraderingen du logger fra. Placer ikke typeskriptfilen i en midlertidig mappe såsom `/tmp` eller `/var/tmp` (filer i disse mapper kan blive slettet under opgraderingen eller under en genstart).

Typeskriptet vil også give dig mulighed for at gennemse information, som er rullet forbi skærmen. Hvis du er ved systemets konsol, så skift til VT2 (med Alt + F2) og efter at du er logget ind, så brug `less -R ~root/upgrade-bullseye.script` for at se filen.

Efter at du har færdiggjort opgraderingen, så kan du stoppe **script** ved at taste `exit` i prompten.

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`.

Hvis du har brugt tilvalget *-t* for **script** så kan du bruge programmet **scriptreplay** for at afspille hele sessionen:

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

4.4.2 Opdatering af pakkelisten

Først skal listen over tilgængelige pakker for den nye udgivelse hentes. Dette gøres ved at køre:

```
# apt update
```

BEMÆRK

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 Sikr dig, at du har tilstrækkelig med plads til opgraderingen

Du skal sikre dig, at du har tilstrækkelig med harddiskplads før du opgraderer med den fulde systemopgradering beskrevet i Afsnit 4.4.5. Først, alle pakker krævet for installation som hentes fra netværket gemmes i `/var/cache/apt/archives` (og undermappen `partial/`, under overførsel), så du skal sikre dig, at du har nok plads på partitionen for filsystemet, som indeholder `/var/` til midlertidigt at hente pakkerne, som skal installeres på dit system. Efter overførslen skal du sikkert bruge ekstra plads i andre filsystempartitioner for både at installere opgraderede pakker (som kan indeholder større binære filer eller mere data) og nye pakker, som vil blive hentet ned for opgraderingen. Hvis dit system ikke har tilstrækkelig med plads, kan du ende med en ufuldstændig opgradering, som det kan være svært at fortryde.

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.
```

BEMÆRK

Kørsel af denne kommando i begyndelsen af opgraderingsprocessen kan medføre en fejl, på grund af årsagerne beskrevet i de næste afsnit. I disse tilfælde skal du vente indtil du har udført den minimale systemopgradering som i Afsnit 4.4.4 før du kører denne kommando for at estimere diskpladsen.

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/.
```

I denne situation, så skab først ledig plads. Du kan:

- 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
  ```

  Du kan også **deborphan**, **debfoster** eller **cruft** ti lat finde redundante pakker. Fjern ikke blindt pakkerne disse værktøjer præsenterer, specielt hvis du bruger aggressive indstillinger, der ikke er standard, som er mere udsat for at give falske positive resultater. Det anbefales stærkt, at du manuelt gennemser pakkerne der bliver foreslået for fjernelse (dvs. deres indhold, størrelse og beskrivelse) før du fjerner dem.
- Remove packages that take up too much space and are not currently needed (you can always reinstall them after the upgrade). If you have `popularity-contest` installed, you can use **popcon-largest-unused** to list the packages you do not use that occupy the most space. You can find the packages that just take up the most disk space with **dpigs** (available in the `debian-goodies` package) or with **wajig** (running `wajig size`). They can also be found with `aptitude`. Start **aptitude** in full-terminal mode, select Views → New Flat Package List, press **l** and enter `~i`, then press **S** and enter `~installsize`. This will give you a handy list to work with.
- Fjern oversættelser og sprogfiler fra system hvis de ikke er krævet. Du kan installere pakken `localepurge` og konfigurere den så at kun nogle få udvalgte sprog bevares i systemet. Dette vil reducere den forbrugt diskplads i `/usr/share/locale`.
- Flyt midlertidigt til et andet system, eller fjern permanent, systemlogge under `/var/log/`.
- Use a temporary `/var/cache/apt/archives`: You can use a temporary cache directory from another filesystem (USB storage device, temporary hard disk, filesystem already in use, ...).

BEMÆRK

Brug ikke en NFS-montering da netværksforbindelsen kan blive afbrudt under opgraderingen.

For eksempel hvis du har et USB-drev monteret på `/media/usbkey`:

1. fjern pakkerne som tidligere er blevet hentet for installation:

```
# apt clean
```

2. kopier mappen `/var/cache/apt/archives` til USB-drevet:

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

3. monter den midlertidige mappe for mellemlageret på den aktuelle:

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

4. efter opgraderingen, gendan den originale `/var/cache/apt/archives`-mappe:

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

5. fjern den tilbageværende `/media/usbkey/archives`.

Du kan oprette den midlertidige mappe for mellemlageret på det filsystem som er monteret på dit system.

- Udfør en minimal opgradering af systemet (se Afsnit 4.4.4) eller delvise opgraderinger af systemet efterfulgt af en fuld opgradering. Dette vil gøre det muligt at opgradere systemet delvist, og give dig mulighed for at rydde pakkemellemlageret før den fulde opgradering.

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

4.4.4 Minimal systemopgradering

VIGTIGT

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

I nogle tilfælde under udførelse af den fulde opgradering (som beskrevet nedenfor) kan der blive fjernet et stort antal pakker, som du måske ønsker at beholde. Vi anbefaler derfor en todelt opgraderingsproces, først en minimal opgradering til at forbigå disse konflikter, og så en fuld opgradering som beskrevet i Afsnit 4.4.5.

For at gøre dette, så kør først:

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

Dette medfører en opgradering af de pakker, som kan opgraderes uden at kærve at andre pakker fjernes eller installeres.

Den mimimale systemopgradering kan også være nyttig når systemet har lidt ledig plads og en fuld opgradering ikke kan køres på grund af pladsbegrænsninger.

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 Opgradering af systemet

Når du har udført de tidligere trin, er du nu klar til at fortsætte med hoveddelen af opgraderingen. Kør:

```
# apt full-upgrade
```

Dette vil udføre en fuldstændig opgradering af systemet, dvs. installere de nyeste tilgængelige versioner af alle pakker, og løse alle eventuelle afhængighedsændringer mellem pakker i forskellige udgivelser. Hvis nødvendigt vil den installere nogle nye pakker (normalt nye biblioteksversioner, eller omdøbte pakker), og fjerne alle forældede pakker der er i konflikt med andre pakker.

When upgrading from a set of CDs/DVDs/BDs, you will probably be asked to insert specific discs at several points during the upgrade. You might have to insert the same disc multiple times; this is due to inter-related packages that have been spread out over the discs.

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 Mulige problemstillinger under opgradering

De følgende afsnit beskriver kendte problemstillinger, som kan opstå under en opgradering til bullseye.

4.5.1 Dist-upgrade fejler med “Kunne ikke udføre øjeblikkelig konfiguration”

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 Forventede fjernelser

Opgraderingsprocessen for bullseye kan anmode om fjernelse af pakker i systemet. Den præcise liste over disse pakker vil variere afhængig af det pakkesæt du har installeret. Disse udgivelsesnoter giver generelle råd om disse fjernelser, men hvis du er i tvivl, så anbefales det, at du undersøger pakkefjernelserne foreslået af hver metode før du fortsætter. For yderligere information om pakker, der er blevet forældet i bullseye, se Afsnit 4.8.

4.5.3 Konflikter eller forhåndsafhængige (Pre-Depends) loop

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
```

for at eliminere nogle af de stridende pakker, eller

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

I ekstreme tilfælde kan det være nødvendigt at fremtvinge reinstallation med en kommando som

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

4.5.4 Filkonflikter

Filkonflikter bør ikke opstå hvis du opgraderer fra et "rent" buster-system, men kan opstå hvis du har uofficielle backports installeret. En filkonflikt vil resultere i en fejl såsom:

```
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>
```

Du kan forsøge at løse en filkonflikt ved med tvang at fjerne pakken nævnt på den *sidste* linje i fejlbeskeden:

```
# 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 Konfigurationsændringer

Under opgraderingen vil du blive stillet nogle spørgsmål angående konfigurationen eller omkonfigurationen af flere pakker. Når du bliver spurgt om en fil i mappen `/etc/init.d` eller filen `/etc/manpath.config` skal erstattes af pakkevedligeholderens version, så er det normalt nødvendigt at svare »ja« for at sikre systemkonsistens. Du kan altid vende tilbage til de ældre versioner, da de bliver gemt med filendelsen `.dpkg-old`.

Hvis du ikke er sikker på, hvad du skal gøre, så skriv navnet på pakken eller filen ned og udred så problemstillingen senere. Du kan søge i typescript-filen for at gennemse informationen på skærmen fra opgraderingen.

4.5.6 Ændring af session til konsol

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.

For at gendanne konsollen hvor opgraderingen var nået til, skal du bruge Ctrl + Alt + F1 (hvis i den grafiske opstartsskærm) eller bruge Alt + F1 (hvis i den lokale konsol for teksttilstand) for at skifte tilbage til den virtuelle terminal 1. Erstat F1 med funktionstasten med det samme antal som den virtuelle terminal opgraderingen kørte i. Du kan også bruge Alt + Venstre piletast eller Alt + Højre piletast for at skifte mellem de forskellige terminaler i teksttilstand.

4.6 Opgradering af din kerne og relaterede pakker

Dette afsnit forklarer hvordan du opgraderer din kerne og identificerer potentielle problemstillinger forbundet med denne opgradering. Du kan enten installere en af `linux-image-*`-pakkerne tilbudt af Debian, eller kompilere en tilpasset kerne fra kilde.

Bemærk at en masse informaton i dette afsnit er baseret på den antagelse, at du vil bruge en af de modulære Debiankerner, sammen med `initramfs-tools` og `udev`. Hvis du vælger at bruge en tilpasset kerne, som ikke kræver en initrd eller hvis du bruger en anden initrd-opretter, kan noget af informationen være urelevant for dig.

4.6.1 Installation af en kernens metapakke

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
```

Hvis du ikke ser et resultat, så skal du installere en ny pakke for linux-image manuelt eller installere en linux-image-metapakke. For at se en liste over tilgængelige metapakker for linux-image, så kør:

```
# 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 Afsnit 5.1.25 before performing the first reboot after the upgrade.

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

4.7 Forberedelse af den næste udgivelse

Efter opgraderingen er der nogle ting, du kan forberede for din næste udgivelse.

- Fjern nye redundante og forældede pakker som beskrevet i Afsnit 4.4.3 og Afsnit 4.8. Du bør gennemgå hvilke konfigurationsfiler de bruger og overveje at fjerne pakkerne, så deres konfigurationsfiler forsvinder. Se også Afsnit 4.7.1.

4.7.1 Fuld fjernelse af afinstallerede pakker

Det er generelt et godt råd at fjerne afinstallerde pakker. Dette gælder specielt hvis de er blevet afinstalleret i en tidligere udgivelsesopgradering f.eks. fra opgraderingen til buster) eller de kom fra en tredjeparts leverandør. Specielt gamle init.d-skripter vides at kunne medføre problemer.

PAS PÅ

Fuld fjernelse af en pakke vil generelt også fjerne logfilerne, så du vil skulle lave en sikkerhedskopi af dem først.

Den følgende kommando viser en liste over alle fjernede pakker, som kan have konfigurationsfiler tilbage på systemet (hvis nogen):

```
# 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 }')
```

Hvis du bruger `aptitude`, så kan du også bruge det følgende alternativ til kommandoerne ovenfor:

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

4.8 Forældede pakker

Introducing lots of new packages, bullseye also retires and omits quite a few old packages that were in buster. It provides no upgrade path for these obsolete packages. While nothing prevents you from continuing to use an obsolete package where desired, the Debian project will usually discontinue security support for it a year after bullseye's release[5], and will not normally provide other support in the meantime. Replacing them with available alternatives, if any, is recommended.

Der kan være mange årsager til at pakker er blevet fjernet fra distributionen: De bliver ikke længere vedligeholdt opstrøms, der er ikke længere en Debianudvikler interesseret i at vedligeholde pakkerne; funktionaliteten de tilbyder er blevet efterfulgt af andre programmer (eller en ny version); eller de anses ikke længere for at være egnet for bullseye på grund af fejl i dem. I det sidste tilfælde, kan pakker stadig være til stede i distributionen "unstable".

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'
```

Debians fejlsporingssystem (`https://bugs.debian.org/`) tilbyder ofte yderligere information om hvorfor pakkerne blev fjernet. Du bør gennemse både de arkiverede fejlrapporter for selve pakken og de arkiverede fejlrapporter for ftp.debian.org pseudo-package (`https://bugs.debian.org/cgi-bin/pkgreport.cgi?pkg=ftp.debian.org&archive=yes`).

For a list of obsolete packages for Bullseye, please refer to Afsnit 5.3.1.

4.8.1 Transitional dummy packages

Some packages from buster may have been replaced in bullseye by transitional dummy packages, which are empty placeholders designed to simplify upgrades. If for instance an application that was formerly a single package has been split into several, a transitional package may be provided with the same name as the old package and with appropriate dependencies to cause the new ones to be installed. After this has happened the redundant dummy package can be safely removed.

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

[5] Eller i den periode hvor der endnu ikke er en ny udgivelse. Typisk er kun to stabile udgivelser understøttet på samme tidspunkt.

Kapitel 5

Ting man skal være opmærksom på i forbindelse med bullseye

Sometimes, changes introduced in a new release have side-effects we cannot reasonably avoid, or they expose bugs somewhere else. This section documents issues we are aware of. Please also read the errata, the relevant packages' documentation, bug reports, and other information mentioned in Afsnit 6.1.

5.1 Upgrade specific items for bullseye

This section covers items related to the upgrade from buster to bullseye.

5.1.1 New VA-API default driver for Intel GPUs

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

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

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

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

5.1.3 Changed security archive layout

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

The security line in your APT configuration may look like:

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

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

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

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

5.1.4 Password hashing uses yescrypt by default

The default password hash for local system accounts has been changed (https://tracker.debian.org/news/1226655/accepted-pam-140-3-source-into-unstable/) from SHA-512 to yescrypt (https://www.openwall.com/yescrypt/) (see crypt(5) (https://manpages.debian.org//bullseye/libcrypt-dev/crypt.5.html)). This is expected to provide improved security against dictionary-based password guessing attacks, in terms of both the space and time complexity of the attack.

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

Old passwords will continue to work using whatever password hash was used to create them.

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

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

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

and replace yescrypt with sha512.

5.1.5 NSS NIS and NIS+ support require new packages

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

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

5.1.6 Config file fragment handling in unbound

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

5.1.7 rsync parameter deprecation

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

5.1.8 Vim addons handling

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

5.1.9 OpenStack and cgroups v1

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

5.1.10 OpenStack API policy files

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

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

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

5.1.11 sendmail downtime during upgrade

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

5.1.12 FUSE 3

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

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

5.1.13 GnuPG options file

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

5.1.14 Linux enables user namespaces by default

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

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

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

```
user.max_user_namespaces = 0
```

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

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

5.1.15 Linux disables unprivileged calls to bpf() by default

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

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

```
kernel.unprivileged_bpf_disabled = 0
```

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

5.1.16 redmine missing in bullseye

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

5.1.17 Exim 4.94

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

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

Typical nonworking examples include:

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

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

  instead of

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

  for a virtual domain alias file.

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

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

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

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

5.1.18 SCSI device probing is non-deterministic

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

5.1.19 rdiff-backup require lockstep upgrade of server and client

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

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

5.1.20 Intel CPU microcode issues

The `intel-microcode` package currently in bullseye and buster-security (see DSA-4934-1 (`https://www.debian.org/security/2021/dsa-4934`)) 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`.

5.1.21 Upgrades involving libgc1c2 need two runs

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

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

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

5.1.23 No new SSH connections possible during upgrade

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

5.1.24 Open vSwitch upgrade requires interfaces(5) change

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

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

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

5.1.25 Ting at gøre efter opgradering og før genstart

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 Begrænsninger i sikkerhedsunderstøttelse

Der er nogle pakker hvor Debian ikke kan love at tilbyde minimale tilbageporteringer for sikkerhedsmæssige problemstillinger. Disse dækkes i de følgende underafsnit.

BEMÆRK

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

5.2.1.1 Security status of web browsers and their rendering engines

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

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

5.2.1.2 OpenJDK 17

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

5.2.1.3 Go-based packages

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

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

5.2.2 Accessing GNOME Settings app without mouse

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

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

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 `sulogin` used since buster, booting with the `rescue` option always requires the root password. If one has not been set, this makes the rescue mode effectively unusable. However it is still possible to boot using the kernel parameter `init=/sbin/sulogin --force`

To configure systemd to do the equivalent of this whenever it boots into rescue mode (also known as single mode: see systemd(1) (`https://manpages.debian.org//bullseye/systemd/systemd.1.html`)), run **sudo systemctl edit rescue.service** and create a file saying just:

```
[Service]
Environment=SYSTEMD_SULOGIN_FORCE=1
```

It might also (or instead) be useful to do this for the `emergency.service` unit, which is started *automatically* in the case of certain errors (see systemd.special(7) (`https://manpages.debian.org//bullseye/systemd/systemd.special.7.html`)), or if `emergency` is added to the kernel command line (e.g. if the system can't be recovered by using the rescue mode).

For background and a discussion on the security implications see #802211 (`https://bugs.debian.org//802211`).

5.3 Obsolescence and deprecation

5.3.1 Værd at bemærke forældede pakker

Den følgende liste viser kendte og værd at bemærke forældede pakker (se Afsnit 4.8 for en beskrivelse).

Listen over forældede pakker inkluderer:

- The `lilo` package has been removed from bullseye. The successor of lilo as boot loader is `grub2`.
- The Mailman mailing list manager suite version 3 is the only available version of Mailman in this release. Mailman has been split up into various components; the core is available in the package `mailman3` and the full suite can be obtained via the `mailman3-full` metapackage.

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

  For upgrading instructions, please see the project's migration documentation. (`https://docs.mailman3.org/en/latest/migration.html`)
- The Linux kernel no longer provides `isdn4linux` (i4l) support. Consequently, the related userland packages `isdnutils`, `isdnactivecards`, `drdsl` and `ibod` have been removed from the archives.
- The deprecated libappindicator libraries are no longer provided. As a result, the related packages `libappindicator1`, `libappindicator3-1` and `libappindicator-dev` are no longer available. This is expected to cause dependency errors for third-party software that still depends on libappindicator to provide system tray and indicator support.

  Debian is using `libayatana-appindicator` as the successor of libappindicator. For technical background see this announcement (`https://lists.debian.org/debian-devel/2018/03/msg00506.html`).
- Debian no longer provides `chef`. If you use Chef for configuration management, the best upgrade path is probably to switch to using the packages provided by Chef Inc (`https://www.chef.io/`).

  For background on the removal, see the removal request (`https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=963750`).
- Python 2 is already beyond its End Of Life, and will receive no security updates. It is not supported for running applications, and packages relying on it have either been switched to Python 3 or removed. However, Debian bullseye does still include a version of Python 2.7, as well as a small

number of Python 2 build tools such as `python-setuptools`. These are present only because they are required for a few application build processes that have not yet been converted to Python 3.

- The `aufs-dkms` package is not part of bullseye. Most `aufs-dkms` users should be able to switch to `overlayfs`, which provides similar functionality with kernel support. However, it's possible to have a Debian installation on a filesystem that is not compatible with `overlayfs`, e.g. `xfs` without `d_type`. Users of `aufs-dkms` are advised to migrate away from `aufs-dkms` before upgrading to bullseye.
- The network connection manager `wicd` will no longer be available after the upgrade, so to avoid the danger of losing connectivity users are recommended to switch before the upgrade to an alternative such as `network-manager` or `connman`.

5.3.2 Deprecated components for bullseye

With the next release of Debian 12 (codenamed bookworm) some features will be deprecated. Users will need to migrate to other alternatives to prevent trouble when updating to Debian 12.

Dette inkluderer de følgende funktioner:

- The historical justifications for the filesystem layout with `/bin`, `/sbin`, and `/lib` directories separate from their equivalents under `/usr` no longer apply today; see the Freedesktop.org summary (`https://www.freedesktop.org/wiki/Software/systemd/TheCaseForTheUsrMerge`). Debian bullseye will be the last Debian release that supports the non-merged-usr layout; for systems with a legacy layout that have been upgraded without a reinstall, the `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`) that were tagged to be ignored in the last part of releasing bullseye can be found in the Debian Bug Tracking System (`https://bugs.debian.org/`). The following bugs were affecting bullseye at the time of the release and worth mentioning in this document:

Bug number	Package (source or binary)	Description
922981 (https://bugs.debian.org/922981)	ca-certificates-java	ca-certificates-java: /etc/ca-certificates/update.d/jks-keystore doesn't update /etc/ssl/certs/java/cacerts
990026 (https://bugs.debian.org/990026)	cron	cron: Reduced charset in MAILTO causes breakage
991081 (https://bugs.debian.org/991081)	gir1.2-diodon-1.0	gir1.2-diodon-1.0 lacks dependencies
990318 (https://bugs.debian.org/990318)	python-pkg-resources	python-pkg-resources: please add Breaks against the unversioned python packages
991449 (https://bugs.debian.org/991449)	fail2ban	fix for CVE-2021-32749 breaks systems with mail from bsd-mailx
990708 (https://bugs.debian.org/990708)	mariadb-server-10.5,galera-4	mariadb-server-10.5: upgrade problems due to galera-3 -> galera-4 switch
980429 (https://bugs.debian.org/980429)	src:gcc-10	g++-10: spurious c++17 mode segmentation fault in append_to_statement_list_1 (tree-iterator.c:65)
980609 (https://bugs.debian.org/980609)	src:gcc-10	missing i386-cpuinfo.h
984574 (https://bugs.debian.org/984574)	gcc-10-base	gcc-10-base: please add Breaks: gcc-8-base (<< 8.4)
984931 (https://bugs.debian.org/984931)	git-el	git-el,elpa-magit: fails to install: /usr/lib/emacsen-common/packages/install/git emacs failed at /usr/lib/emacsen-common/lib.pl line 19, <TSORT> line 7.
987264 (https://bugs.debian.org/987264)	git-el	git-el: fails to install with xemacs21
991082 (https://bugs.debian.org/991082)	gir1.2-gtd-1.0	gir1.2-gtd-1.0 has empty Depends
948739 (https://bugs.debian.org/948739)	gparted	gparted should not mask .mount units
984714 (https://bugs.debian.org/984714)	gparted	gparted 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 filesystem

Bug number	Package (source or binary)	Description
981054 (https://bugs.debian.org/981054)	openipmi	openipmi: Missing dependency on kmod
948318 (https://bugs.debian.org/948318)	openssh-server	openssh-server: Unable to restart sshd restart after upgrade to version 8.1p1-2
991151 (https://bugs.debian.org/991151)	procps	procps: dropped the reload option from the init script, breaking corekeeper
989103 (https://bugs.debian.org/989103)	pulseaudio	pulseaudio regressed on control = Wave configuration
984580 (https://bugs.debian.org/984580)	libpython3.9-dev	libpython3.9-dev: missing dependency on zlib1g-dev
990417 (https://bugs.debian.org/990417)	src:qemu	openjdk-11-jre-headless: running java in qemu s390 gives a SIGILL at C [linux-vdso64.so.1 + 0x6f8] _kernel_getcpu + 0x8
859926 (https://bugs.debian.org/859926)	speech-dispatcher	breaks with pulse-audio as output when spawned by speechd-up from init system
932501 (https://bugs.debian.org/932501)	src:squid-deb-proxy	squid-deb-proxy: daemon does not start due to the conf file not being allowed by apparmor
991588 (https://bugs.debian.org/991588)	tpm2-abrmd	tpm2-abrmd should not use Requires = systemd-udev-settle.service in its unit
991939 (https://bugs.debian.org/991939)	libjs-bootstrap4	libjs-bootstrap4: broken symlinks: /usr/share/javascript/bootstrap4/css/bootstrap*.css.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

Kapitel 6

Yderligere oplysninger om Debian

6.1 Yderligere læsning

Beyond these release notes and the installation guide, further documentation on Debian is available from the Debian Documentation Project (DDP), whose goal is to create high-quality documentation for Debian users and developers, such as the Debian Reference, Debian New Maintainers Guide, the Debian FAQ, and many more. For full details of the existing resources see the Debian Documentation website (`https://www.debian.org/doc/`) and the Debian Wiki (`https://wiki.debian.org/`).

Dokumentationen for enkelte pakker installeres i `/usr/share/doc/`*`pakke`*. Dette kan omfatte oplysninger om ophavsret, Debian-specifikke detaljer samt dokumentation fra programmets ophavssted.

6.2 Få hjælp

There are many sources of help, advice, and support for Debian users, though these should only be considered after researching the issue in available documentation. This section provides a short introduction to these sources which may be helpful for new Debian users.

6.2.1 E-post-lister

De mest interessante e-post-lister til Debianbrugere er den engelske liste debian-user plus listerne debian-user-*`sprog`* for andre sprog (den danske er `debian-user-danish`). Oplysninger om disse lister og hvordan man abonnerer på dem kan findes på `https://lists.debian.org/`. Se venligst i arkiverne om dit spørgsmål allerede er besvaret, før du skriver, og følg i øvrigt standard-etiketten for e-post-lister.

6.2.2 Internet Relay Chat

Debian has an IRC channel dedicated to support and aid for Debian users, located on the OFTC IRC network. To access the channel, point your favorite IRC client at irc.debian.org and join `#debian`.

Følg kanalens retningslinjer og udvis respekt for andre brugere. Retningslinjerne kan findes på Debians wiki (`https://wiki.debian.org/DebianIRC`).

Yderligere oplysninger om OFTC kan findes på websiden (`http://www.oftc.net/`).

6.3 Fejlrapportering

We strive to make Debian a high-quality operating system; however that does not mean that the packages we provide are totally free of bugs. Consistent with Debian's "open development" philosophy and as a service to our users, we provide all the information on reported bugs at our own Bug Tracking System (BTS). The BTS can be browsed at `https://bugs.debian.org/`.

Hvis du finder en fejl i distributionen eller i de programpakker, som er en del af den, så rapporter dem venligst så de kan blive rettet i fremtidige udgivelser. Fejlrapportering kræver en gyldig e-postadresse. Vi beder om dette for, at vi kan spore fejlrapporterne, og så udviklerne kan kontakte ophavspersonen hvis der kræves flere oplysninger.

You can submit a bug report using the program **reportbug** or manually using e-mail. You can find out more about the Bug Tracking System and how to use it by reading the reference documentation (available at `/usr/share/doc/debian` if you have `doc-debian` installed) or online at the Bug Tracking System (`https://bugs.debian.org/`).

6.4 Bidrag til Debian

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

Hvis du kan afsætte mere tid, kan du håndtere et stykke af Debians fri softwaresamling. Det er især en hjælp hvis folk tager ansvaret for eller vedligeholder ting, hvis inklusion i Debian forespørges af andre. Databasen Work Needing and Prospective Packages (`https://www.debian.org/devel/wnpp/`) indeholder denne type oplysninger. Hvis du er interesseret i specifikke grupper, vil du måske finde det underholdende at bidrage til nogle af Debians underprojekter (`https://www.debian.org/devel/#projects`), inklusive portering til bestemte arkitekturer og Debian Pure Blends (`https://wiki.debian.org/DebianPureBlends`) for specifikke brugergrupper, blandt mange andre.

Under alle omstændigheder: Hvis du på nogen måde arbejder inden for den frie programbevægelse, enten som bruger, programmør, dokumentationsforfatter eller oversætter, hjælper du allerede de frie programmer. At bidrage er både lønsomt og morsomt, lader dig møde nye mennesker, og giver dig en rar fornemmelse indeni.

Kapitel 7

Ordliste

ACPI
: Advanced Configuration and Power Interface

ALSA
: Advanced Linux Sound Architecture (avanceret lydarkitektur for Linux)

BD
: blu-ray-disk

cd
: Compact Disc

cd-rom
: Compact Disc Read Only Memory

DHCP
: Dynamic Host Configuration Protocol (konfigurationsprotokol for dynamisk vært)

DLBD
: Dual Layer Blu-ray Disc

DNS
: Domain Name System (domænenavnsystem)

dvd
: Digital Versatile Disc

GIMP
: GNU Image Manipulation Program (billedbehandlingsprogrammet GIMP)

GNU
: GNU's Not Unix (GNU er ikke Unix)

GPG
: GNU Privacy Guard

LDAP
: Lightweight Directory Access Protocol

LSB
: Linux Standard Base

LVM
: Logical Volume Manager (logisk diskenhedshåndtering)

MTA
: Mail Transport Agent (postbehandlingsagent)

NBD
: Network Block Device (netværksblokenhed)

NFS
: Network File System (netværksfilsystem)

NIC
: Network Interface Card (netværksgrænsefladekort)

NIS
: Network Information Service (netværksinformationstjeneste)

PHP
: PHP: Hypertext Preprocessor

RAID
: Redundant Array of Independent Disks

SATA
: Serial Advanced Technology Attachment

SSL
: Secure Sockets Layer (sikkert sokkellag)

TLS
: Transport Layer Security (sikkerhed for transportlag)

UEFI
: Unified Extensible Firmware Interface

USB
: Universal Serial Bus

UUID
: Universally Unique Identifier

WPA
: Wi-Fi Protected Access (Wi-Fi-beskyttet adgang)

Bilag A

Håndter dit buster-system før opgraderingen

Dette bilag indeholder information om, hvordan du kontrollerer, at du kan installere eller opgradere pakker fra buster inden du opgraderer til bullseye. Dette bør kun være nødvendigt i specifikke situationer.

A.1 Opgradering af dit buster-system

Det er grundlæggende ikke forskelligt fra enhver anden opgradering af buster som du har udført. Den eneste forskel er, at du først skal sikre dig, at din pakkeliste stadig indeholder referencer til buster som forklaret i Afsnit A.2.

Hvis du opgraderer dit system via et Debianspejl, vil systemet automatisk blive opgraderet til den seneste punktudgave (point release) af 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.

Hvis du allerede har installeret pakker fra bullseye, er der ikke længere meget mening i at installere pakker fra buster. I dette tilfælde skal du bestemme dig for, om du vil fortsætte eller ej. Det er muligt at nedgradere pakker, men det beskrives ikke her.

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.

VIGTIGT

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.

Hvis du har foretaget ændringer, så gem filen og kør

```
# apt update
```

for at opdatere pakkelisten.

A.3 Fjerner forældede konfigurationsfiler

Før du opgraderer dit system til bullseye, så anbefales det at fjerne gamle konfigurationsfiler (såsom `*.dpkg-{new,old}`-filer under `/etc` fra systemet.

Bilag B

Bidragydere til udgivelsesnoterne

Mange har hjulpet til med udgivelsesnoterne, blandt andre

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, och W. Martin Borgert.

Dette dokument er oversat til mange sprog. Mange tak til alle oversætterne!

Oversat til dansk af: Joe Hansen, Torben Grøn Helligsø, Morten Bo Johansen, Ask Hjorth Larsen, Nicky Thomassen.

Indeks