Udgivelsesnoter til Debian 10 (buster), 64-bit ARM

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

16. december 2022

Indhold

v

Kapitel 1

Introduktion

Dette dokument informerer brugere af Debian-distributionen om større ændringer i version 10 (kodenavn buster).

Udgivelsesnoterne har information om, hvordan du sikkert opgraderer fra version 9 (kodenavn stretch) til den aktuelle udgave og informerer brugere om kendte problemstillinger, som kan opstå under opgraderingen.

Du kan se den seneste version af dette dokument på https://www.debian.org/releases/buster/releasenotes. Du kan sikre dig, at du læser den seneste version af dokumentet ved at tjekke datoen på den første side.

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 stretch). Hvis du har brug for at opgradere fra en ældre version, foreslår vi, at du læser tidligere udgaver af udgivelsesnoterne og først opgraderer til stretch.

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 stretch til buster. 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 10

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

2.1 Understøttede arkitekturer

Følgende er de officielt understøttede arkitekturer i Debian 10:

- 32-bit pc (`i386`) og 64-bit pc (`amd64`)

- 64-bit ARM (`arm64`)

- ARM EABI (`armel`)

- ARMv7 (EABI hard-float ABI, `armhf`)

- MIPS (`mips` (big endian) og `mipsel` (little endian))

- 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 stretch. Distributionen indeholder over 13370 nye pakker, og i alt 57703 pakker. De fleste programmer i distributionen er blevet opdateret: over 35532 softwarepakker (dette svarer til 62 % af alle pakker i stretch). Et betydeligt antal pakker (over 7278, 13 % af alle pakker i stretch) 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.

Debian again ships with several desktop applications and environments. Among others it now includes the desktop environments GNOME 3.30, KDE Plasma 5.14, LXDE 10, LXQt 0.14, MATE 1.20, and Xfce 4.12.

Produktivitetsprogrammer er også blevet opgraderet, inklusive kontorpakkerne:

- LibreOffice is upgraded to version 6.1;

- Calligra is upgraded to 3.1.

- GNUcash is upgraded to 3.4;

With buster, Debian for the first time brings a mandatory access control framework enabled per default. New installations of Debian buster will have AppArmor installed and enabled per default. See below for more information.

Besides, buster is the first Debian release to ship with Rust based programs such as Firefox, ripgrep, fd, exa, etc. and a significant number of Rust based libraries (more than 450). Buster ships with Rustc 1.34.

Updates of other desktop applications include the upgrade to Evolution 3.30.

Blandt meget andet inkluderer denne udgave følgende opdateringer:

Pakker	Version i 9 (stretch)	Version i 10 (buster)
Apache	2.4.25	2.4.38
BIND DNS-server	9.10	9.11
Cryptsetup	1.7	2.1
Dovecot MTA	2.2.27	2.3.4
Emacs	24.5 and 25.1	26.1
Exim som standard-e-postserver	4.89	4.92
GNU Compiler Collection som standardcompiler	6.3	7.4 and 8.3
GIMP	2.8.18	2.10.8
GnuPG	2.1	2.2
Inkscape	0.92.1	0.92.4
GNU C-programbiblioteket	2.24	2.28
lighttpd	1.4.45	1.4.53
Linux-kerneaftryk	4.9 series	4.19 series
LLVM/Clang toolchain	3.7	6.0.1 and 7.0.1 (default)
MariaDB	10.1	10.3
Nginx	1.10	1.14
OpenJDK	8	11
OpenSSH	7.4p1	7.9p1
Perl	5.24	5.28
PHP	7.0	7.3
Postfix MTA	3.1.8	3.3.2
PostgreSQL	9.6	11
Python 3	3.5.3	3.7.3
Rustc		1.34
Samba	4.5	4.9
Vim	8.0	8.1

2.2.1   UEFI Secure Boot

Secure Boot is a feature enabled on most PCs that prevents loading unsigned code, protecting against some kinds of bootkit and rootkit.

Debian can now be installed and run on most PCs with Secure Boot enabled.

It is possible to enable Secure Boot on a system that has an existing Debian installation, if it already boots using UEFI. Before doing this, it's necessary to install `shim-signed`, `grub-efi-amd64-signed` or `grub-efi-ia32-signed`, and a Linux kernel package from buster.

Some features of GRUB and Linux are restricted in Secure Boot mode, to prevent modifications to their code.

More information can be found on the Debian wiki at SecureBoot (`https://wiki.debian.org/SecureBoot`).

2.2.2   AppArmor enabled per default

Debian buster has `AppArmor` enabled per default. `AppArmor` is a mandatory access control framework for restricting programs' capabilities (such as mount, ptrace, and signal permissions, or file read, write, and execute access) by defining per-program profiles.

The `apparmor` package ships with AppArmor profiles for several programs. Some other packages, such as `evince`, include profiles for the programs they ship. More profiles can be found in the `apparmor-profiles-extra` package.

AppArmor is pulled in due to a `Recommends` by the buster Linux kernel package. On systems that are configured to not install recommended packages by default, the `apparmor` package can be installed manually in order to enable `AppArmor`.

2.2.3 Optional hardening of APT

All methods provided by APT (e.g. http, and https) except for cdrom, gpgv, and rsh can make use of seccomp-BPF sandboxing as supplied by the Linux kernel to restrict the list of allowed system calls, and trap all others with a `SIGSYS` signal. This sandboxing is currently opt-in and needs to be enabled with:

```
APT::Sandbox::Seccomp is a boolean to turn it on/off
```

Two options can be used to configure this further:

```
APT::Sandbox::Seccomp::Trap is a list of names of more syscalls to trap
APT::Sandbox::Seccomp::Allow is a list of names of more syscalls to allow
```

2.2.4 Unattended-upgrades for stable point releases

Previous versions of `unattended-upgrades` defaulted to installing only upgrades that came from the security suite. In buster it now also automates upgrading to the latest stable point release. For details, see the package's NEWS.Debian file.

2.2.5 Substantially improved man pages for German speaking users

The documentation (`man`-pages) for several projects like `systemd`, `util-linux` and `mutt` has been substantially extended. Please install `manpages-de` to benefit from the improvements. During the lifetime of buster further new/improved translations will be provided within the `backports` archive.

2.2.6 Network filtering based on nftables framework by default

Starting with `iptables` v1.8.2 the binary package includes `iptables-nft` and `iptables-legacy`, two variants of the `iptables` command line interface. The nftables-based variant, using the `nf_tables` Linux kernel subsystem, is the default in buster. The legacy variant uses the `x_tables` Linux kernel subsystem. The `update-alternatives` system can be used to select one variant or the other.

This applies to all related tools and utilities:

- iptables

- iptables-save

- iptables-restore

- ip6tables

- ip6tables-save

- ip6tables-restore

- arptables

- arptables-save

- arptables-restore

- ebtables

- ebtables-save

- ebtables-restore

All these have also gained `-nft` and `-legacy` variants. The `-nft` option is for users who can't or don't want to migrate to the native `nftables` command line interface. However, users are strongly enouraged to switch to the `nftables` interface rather than using `iptables`.

`nftables` provides a full replacement for `iptables`, with much better performance, a refreshed syntax, better support for IPv4/IPv6 dual-stack firewalls, full atomic operations for dynamic ruleset updates, a Netlink API for third party applications, faster packet classification through enhanced generic set and map infrastructures, and many other improvements (`https://wiki.nftables.org`).

This change is in line with what other major Linux distributions are doing, such as RedHat, which now uses `nftables` as its default firewalling tool (`https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8-beta/html-single/8.0_beta_release_notes/index#networking_2`).

Also, please note that all `iptables` binaries are now installed in `/usr/sbin` instead of `/sbin`. A compatibility symlink is in place, but will be dropped after the buster release cycle. Hardcoded paths to the binaries in scripts will need to be corrected and are worth avoiding.

Extensive documentation is available in the package's README and NEWS files and on the Debian Wiki (`https://wiki.debian.org/nftables`).

2.2.7 Cryptsetup defaults to on-disk LUKS2 format

The `cryptsetup` version shipped with Debian buster uses the new on-disk `LUKS2` format. New `LUKS` volumes will use this format by default.

Unlike the previous `LUKS1` format, `LUKS2` provides redundancy of metadata, detection of metadata corruption, and configurable `PBKDF` algorithms. Authenticated encryption is supported as well, but still marked as experimental.

Existing `LUKS1` volumes will not be updated automatically. They can be converted, but not all `LUKS2` features will be available due to header size incompatibilities. See the cryptsetup (`https://manpages.debian.org/buster/cryptsetup`) manpage for more information.

Please note that the GNU GRUB bootloader doesn't support the `LUKS2` format yet. See the corresponding documentation (`https://cryptsetup-team.pages.debian.net/cryptsetup/encrypted-boot.html`) for further information on how to install Debian 10 with encrypted boot.

2.2.8 Driverless printing with CUPS 2.2.10

Debian 10 provides CUPS 2.2.10 and `cups-filters` 1.21.6. Together these give a user everything that is needed to take advantage of driverless printing (`https://wiki.debian.org/DriverlessPrinting`). The principal requirement is that a network print queue or printer offers an AirPrint service. A modern IPP printer is highly likely to be AirPrint-capable; a Debian CUPS print queue is always AirPrint-enabled.

In essence, the DNS-SD (Bonjour) broadcasts from a CUPS server advertising a queue, or those from IPP printers, are capable of being displayed in the print dialogs of applications without any action being required on the part of a user. An additional benefit is that the use of non-free vendor printing drivers and plugins can be dispensed with.

A default installation of the `cups` package also installs the package `cups-browsed`; print queues and IPP printers will now be automatically set up and managed by this utility. This is the recommended way (`https://wiki.debian.org/QuickPrintQueuesCUPS`) for a user to experience seamless and trouble-free driverless printing.

2.2.9 Basic support for Allwinner A64 based devices

Thanks to the efforts of the linux-sunxi community (`https://linux-sunxi.org`) Debian buster will have basic suport for many devices based on the Allwinner A64 SoC. This includes FriendlyARM NanoPi A64; Olimex A64-OLinuXino and TERES-A64; PINE64 PINE A64/A64+/A64-LTS, SOPINE, and Pinebook; SINOVOIP Banana Pi BPI-M64; and Xunlong Orange Pi Win(Plus).

The essential features of these devices (e.g. serial console, ethernet, USB ports and basic video output) should work with the kernel from buster. More advanced features (e.g. audio or accelerated video) are included or scheduled to be included in later kernels, which will be made available as usual through the backports archive (`https://backports.debian.org`). See also the status page (`https://linux-sunxi.org/Linux_mainlining_effort`) for the Linux mainlining effort.

2.2.10   News from Debian Med Blend

The Debian Med team has added several new packages and updates for software targeting life sciences and medicine. The effort to add Continuous Integration support for the packages in this field was (and will be) continued.

To install packages maintained by the Debian Med team, install the metapackages named `med-*`, which are at version 3.3 for Debian buster. Feel free to visit the Debian Med tasks pages (`http://blends.debian.org/med/tasks`) to see the full range of biological and medical software available in Debian.

2.2.11   GNOME defaults to Wayland

Following upstream, GNOME in buster defaults to using the Wayland display server instead of Xorg. Wayland has a simpler and more modern design, which has advantages for security.

The Xorg display server is still installed by default and the default display manager still allows you to choose it as the display server for the next session, which may be needed if you want to use some applications (see Afsnit 5.1.9).

People requiring accessibility features of the display server, e.g. global keyboard shortcuts, are recommended to use Xorg instead of Wayland.

2.2.12   Merged /usr on fresh installs

On fresh installs, the content of `/bin`, `/sbin` and `/lib` will be installed into their `/usr` counterpart by default. `/bin`, `/sbin` and `/lib` will be soft-links pointing at their directory counterpart under `/usr/`. In graphical form:

```
/bin b''→b'' /usr/bin
/sbin b''→b'' /usr/sbin
/lib b''→b'' /usr/lib
```

When upgrading to buster, systems are left as they are, although the `usrmerge` package exists to do the conversion if desired. The freedesktop.org (`https://www.freedesktop.org`) project hosts a Wiki (`https://www.freedesktop.org/wiki/Software/systemd/TheCaseForTheUsrMerge/`) with most of the rationale.

This change shouldn't impact normal users that only run packages provided by Debian, but it may be something that people that use or build third party software want to be aware of.

2.2.13   News from Debian Live team

The Debian Live team is proud to introduce LXQt live ISOs as a new flavor. LXQt is a lightweight Qt desktop environment. It will not get in your way. It will not hang or slow down your system. It is focused on being a classic desktop with a modern look and feel.

The LXQt desktop environment offered in the Debian Live LXQt project is pure, unmodified, so you will get the standard desktop experience that the LXQt developers created for their popular operating system. Users are presented with the standard LXQt layout comprised of a single panel (taskbar) located on the bottom edge of the screen, which includes various useful applets, such as the Main Menu, task manager, app launcher, system tray area, and integrated calendar.

The buster live images come with something new that a bunch of other distributions have also adopted, which is the Calamares installer. Calamares is an independent installer project (they call it "The universal installer framework") which offers a Qt based interface for installing a system. It doesn't replace debian-installer on the live images; rather, it serves a different audience.

Calamares is really easy to use, with friendly guided partitioning and really simple full-disk encryption setup. It doesn't cover all the advanced features of debian-installer (although it very recently got RAID support) and it doesn't have an unattended install mode either. However, for 95%+ of desktop and laptop users, Calamares is a much easier way to get a system installed, which makes it very appropriate for live systems. For anyone who needs anything more complicated, or who's doing a mass-install, debian-installer is still available in both text and GUI forms.

Debian Live Buster re-introduces the standard live image. This is a basic Debian image that contains a base Debian system without any graphical user interface. Because it installs from a squashfs image

rather than installing the system files using **dpkg**, installation times are a lot faster than installing from a minimal Debian installation image.

Kapitel 3

Installeringssystemet

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

Aftryk af installeringsprogrammet til buster kan findes sammen med installeringsguiden på Debians hjemmeside (`https://www.debian.org/releases/buster/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/buster/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 9, resulting in improved hardware support and some exciting new features or improvements.

Most notably there is the initial support for UEFI Secure Boot (see Afsnit 2.2.1), which has been added to the installation images.

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

3.1.1   Automatisk installering

Nogle ændringer som er nævnt ovenover indebærer også ændringer i understøttelsen af automatisk installering med forindstillede filer. Dette betyder at hvis du har forindstillede filer, der fungerede med installeringsprogrammet til stretch, så kan du ikke forvente at disse fungerer med det nye installerings-program, uden at de redigeres.

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

Kapitel 4

Opgraderinger fra Debian 9 (stretch)

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 buster, 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 risiko 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 buster 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/buster/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 image or a Linux live CD. 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.

4.1.6 Verify network interface name support

Systems upgraded from older releases that still use network interfaces with names like `eth0` or `wlan0` are at risk of losing networking once they switch to buster; see Afsnit 5.1.6 for migration instructions.

4.2 Checking APT configuration status

The upgrade process described in this chapter has been designed for "pure" Debian stable systems. If your APT configuration mentions additional sources besides stretch, 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/buster//buster/apt/sources.list.5.html`). If your system is using multiple source-list files then you will need to ensure they stay consistent.

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 '~i(!~ODebian)'
$ apt-forktracer | sort
```

Direct upgrades from Debian releases older than 9 (stretch) are not supported. Please follow the instructions in the Release Notes for Debian 9 (`https://www.debian.org/releases/stretch/releasenotes`) to upgrade to Debian 9 first.

Denne procedure antager også, at dit sytem er blevet opdateret til den sidste punktversion af stretch. Hvis du ikke har udført dette eller er usikker, så følg instruktionerne i Afsnit A.1.

You should also 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 *stretch* and not to *stable* or *buster*; see Afsnit A.2.

It is a good idea to remove obsolete packages from your system before upgrading.

4.2.1 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.

4.2.2 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 buster 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 stretch-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.

4.2.3 Deaktivering af APT-pinning

Hvis du har konfigureret APT til at installere bestemte pakker fra en distribution udover stable (f.eks. fra testing), så skal du måske ændre din APT-pinnings konfiguration (gemt i `/etc/apt/preferences`) for at tillade pakkeopgraderinger af versioner i den nye stabile version. Yderligere information om APT-pinning kan findes i apt_preferences(5).

4.2.4 Kontrol af pakkestatus

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 stretch as explained in Afsnit A.2.

---

[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.

4.3 Preparing APT source-list files

Before starting the upgrade you must reconfigure APT's source-list files (`/etc/apt/sources.list` and files under `/etc/apt/sources.list.d/`).

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. `stretch`, `buster`) 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 `buster` changes from e.g. `stable` to `oldstable`.

- 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 buster 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/buster/main/binary-arm64/...
http://mirrors.kernel.org/debian/dists/buster/contrib/binary-arm64/...
```

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 buster 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/buster/main/binary-arm64/...
    /var/local/debian/dists/buster/contrib/binary-arm64/...
```

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

```
deb file:/var/local/debian buster 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 "`buster`" or to "`stable`". There should not be any sources entries pointing to stretch.

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 opgraderings-sessionen. 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-busterstep.time -a ~/upgrade-busterstep.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-buster.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-busterstep.time ~/upgrade-busterstep.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 systemop-gradering 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 stretch 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 /media/usbkey/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 stretch as described in Afsnit A.2.

4.4.4 Minimal systemopgradering

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-get upgrade
```

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 buster.

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 stretch and buster sources to your APT source-list files and run **apt update**.

4.5.2   Forventede fjernelser

Opgraderingsprocessen for buster 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 buster, 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" stretch-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 stretch to buster, 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 5.1.12 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 stretch) 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, buster also retires and omits quite a few old packages that were in stretch. 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 buster'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 buster 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:

---

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

```
# 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 Buster, please refer to Afsnit 5.1.10.

4.8.1 Transitional dummy packages

Some packages from stretch may have been replaced in buster 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.

Kapitel 5

Ting man skal være opmærksom på i forbindelse med buster

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 buster

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

5.1.1 Hidepid mount option for procfs unsupported

Using the `hidepid` mount option for `/proc` is known to cause problems with current versions of systemd, and is considered by systemd upstream to be an unsupported configuration. Users who have modified `/etc/fstab` to enable this option are advised to disable it before the upgrade, to ensure login sessions work on buster. (A possible route to re-enabling it is outlined on the wiki's Hardening (https://wiki.debian.org/Hardening#Mounting_.2Fproc_with_hidepid) page.)

5.1.2 ypbind fails to start with -no-dbus

The default options of `ypbind` have changed. However, if you have modified this file the old default will not be updated and you must make sure that the `YPBINDARGS=` option in `/etc/default/nis` does not include `-no-dbus`. With `-no-dbus` present, **ypbind** will fail to start, and you may not be able to log in. For more info see bug #906436 (https://bugs.debian.org/906436).

5.1.3 NIS server does not answer NIS client requests by default

The default behavior of `rpcbind` has changed to no longer answer remote calls from NIS clients. On NIS servers you will need to add the (Debian-specific) `-r` flag to the command line options of **rpcbind**, otherwise users will not be able to log into your NIS client machines. For more info see bug #935492 (https://bugs.debian.org/935492).

5.1.4 sshd fails to authenticate

The semantics of `PubkeyAcceptedKeyTypes` and the similar `HostbasedAcceptedKeyTypes` options for `sshd` have changed. These now specify signature algorithms that are accepted for their respective authentication mechanism, where previously they specified accepted key types. This distinction matters when using the RSA/SHA2 signature algorithms `rsa-sha2-256`, `rsa-sha2-512` and their certificate counterparts. Configurations that override these options but omit these algorithm names may cause unexpected authentication failures.

No action is required for configurations that accept the default for these options.

5.1.5 Daemons fail to start or system appears to hang during boot

Due to `systemd` needing entropy during boot and the kernel treating such calls as blocking when available entropy is low, the system may hang for minutes to hours until the randomness subsystem is sufficiently initialized (`random: crng init done`). For `amd64` systems supporting the `RDRAND` instruction this issue is avoided by the Debian kernel using this instruction by default (`CONFIG_RANDOM_TRUST_CPU`).

Non-`amd64` systems and some types of virtual machines need to provide a different source of entropy to continue fast booting. `haveged` has been chosen for this within the Debian Installer project and may be a valid option if hardware entropy is not available on the system. On virtual machines consider forwarding entropy from the host to the VMs via `virtio_rng`.

If you read this after upgrading a remote system to buster, ping the system on the network continuously as this adds entropy to the randomness pool and the system will eventually be reachable by ssh again.

See the wiki (`https://wiki.debian.org/BoottimeEntropyStarvation`) and DLange's overview of the issue (`https://daniel-lange.com/archives/152-hello-buster.html`) for other options.

5.1.6 Migrating from legacy network interface names

If your system was upgraded from an earlier release, and still uses the old-style network interface names that were deprecated with stretch (such as `eth0` or `wlan0`), you should be aware that the mechanism of defining their names via `/etc/udev/rules.d/70-persistent-net.rules` is officially not supported by `udev` in buster (while it may still work in some cases). To avoid the danger of your machine losing networking after the upgrade to buster, it is recommended that you migrate in advance to the new naming scheme (usually meaning names like `enp0s1` or `wlp2s5`, which incorporate PCI bus- and slot-numbers). Take care to update any interface names hard-coded in configuration for firewalls, `ifupdown`, and so on.

The alternative is to switch to a supported mechanism for enforcing the old naming scheme, such as a systemd `.link` file (see systemd.link(5) (`https://manpages.debian.org/buster/systemd.link`)). The `net.ifnames=0` kernel commandline option might also work for systems with only one network interface (of a given type).

To find the new-style names that will be used, first find the current names of the relevant interfaces:

```
$ echo /sys/class/net/[ew]*
```

For each of these names, check whether it is used in configuration files, and what name `udev` would prefer to use for it:

```
$ sudo rgrep -w eth0 /etc
$ udevadm test-builtin net_id /sys/class/net/eth0 2>/dev/null
```

This should give enough information to devise a migration plan. (If the `udevadm` output includes an "onboard" or "slot" name, that takes priority; MAC-based names are normally treated as a fallback, but may be needed for USB network hardware.)

Once you are ready to carry out the switch, disable `70-persistent-net.rules` either by renaming it or by commenting out individual lines. On virtual machines you will need to remove the files `/etc/systemd/network/99-default.link` and (if using virtio network devices) `/etc/systemd/network/50-virtio-kernel-names.link`. Then rebuild the `initrd`:

```
$ sudo update-initramfs -u
```

and reboot. Your system should now have new-style network interface names. Adjust any remaining configuration files, and test your system.

See the wiki (`https://wiki.debian.org/NetworkInterfaceNames`), upstream documentation (`https://www.freedesktop.org/software/systemd/man/systemd.net-naming-scheme.html`), and the `udev` `README.Debian` for further information.

5.1.7 Module configuration for bonding and dummy interfaces

Systems using channel bonding and/or dummy interfaces, for instance to configure a machine as a router, may encounter problems upgrading to buster. New versions of `systemd` install a file `/lib/`

`modprobe.d/systemd.conf` (intended to simplify configuration via **systemd-networkd**) which contains the lines

```
options bonding max_bonds=0
options dummy numdummies=0
```

Admins who were depending on different values will need to ensure they are set in the correct way to take precedence. A file in `/etc/modprobe.d` will override one with the same name under `/lib/modprobe.d`, but the names are processed in alphabetical order, so `/lib/modprobe.d/systemd.conf` follows and overrides (for instance) `/etc/modprobe.d/dummy.conf`. Make sure that any local configuration file has a name that sorts after "`systemd.conf`", such as "`/etc/modprobe.d/zz-local.conf`".

5.1.8   OpenSSL default version and security level raised

Following various security recommendations, the default minimum TLS version has been changed from TLSv1 to TLSv1.2.

The default security level for TLS connections has also been increased from level 1 to level 2. This moves from the 80 bit security level to the 112 bit security level and will require 2048 bit or larger RSA and DHE keys, 224 bit or larger ECC keys, and SHA-2.

The system wide settings can be changed in `/etc/ssl/openssl.cnf`. Applications might also have an application specific way to override the defaults.

In the default `/etc/ssl/openssl.cnf` there is a `MinProtocol` and `CipherString` line. The `CipherString` can also set the security level. Information about the security levels can be found in the SSL_CTX_set_security_level(3ssl) (`https://manpages.debian.org/buster/SSL_CTX_set_security_level(3ssl)`) manpage. The list of valid strings for the minimum protocol version can be found in SSL_CONF_cmd(3ssl) (`https://manpages.debian.org/buster/SSL_CONF_cmd(3ssl)`). Other information can be found in ciphers(1ssl) (`https://manpages.debian.org/buster/ciphers(1ssl)`) and config(5ssl) (`https://manpages.debian.org/buster/config(5ssl)`).

Changing the system wide defaults in `/etc/ssl/openssl.cnf` back to their previous values can be done by setting:

```
        MinProtocol = None
        CipherString = DEFAULT
```

It's recommended that you contact the remote site if the defaults cause problems.

5.1.9   Some applications don't work in GNOME on Wayland

GNOME in buster has changed its default display server from Xorg to Wayland (see Afsnit 2.2.11). Some applications, including the popular package manager `synaptic`, the default Simplified Chinese input method, `fcitx`, and most screen recording applications, have not been updated to work properly under Wayland. In order to use these packages, one needs to log in with a `GNOME on Xorg` session.

5.1.10   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 package `mcelog` is no longer supported with kernel versions above 4.12. `rasdaemon` can be used as its replacement.

- The package `revelation`, which is used to store passwords, is not included in buster. `keepass2` can import previously exported password XML files from `revelation`. Please make sure you export your data from revelation before upgrading, to avoid losing access to your passwords.

- The package `phpmyadmin` is not included in buster.

- `ipsec-tools` and `racoon` have been removed from buster as their source has been lagging behind in adapting to new threats.

  Users are encouraged to migrate to `libreswan`, which has broader protocol compatibility and is being actively maintained upstream.

`libreswan` should be fully compatible in terms of communication protocols since it implements a superset of `racoon`'s supported protocols.

- The simple MTA `ssmtp` has been dropped for buster. This is due to it currently not validating TLS certs; see bug #662960 (`https://bugs.debian.org/662960`).

- The `ecryptfs-utils` package is not part of buster due to an unfixed serious bug (#765854 (`https://bugs.debian.org/765854`)). At the time of writing this paragraph, there was no clear advice for users of eCryptfs, except not to upgrade.

5.1.11   Deprecated components for buster

With the next release of Debian 11 (codenamed bullseye) some features will be deprecated. Users will need to migrate to other alternatives to prevent trouble when updating to Debian 11.

Dette inkluderer de følgende funktioner:

- Python 2 will stop being supported by its upstream on January 1, 2020 (`https://www.python.org/dev/peps/pep-0373/`). Debian hopes to drop `python-2.7` for Debian 11. If users have functionality that relies on **python**, they should prepare to migrate to **python3**.

- Icinga 1.x is EOL upstream since 2018-12-31; while the `icinga` package is still present, users should use the buster lifetime to migrate to Icinga 2 (`icinga2` package) and Icinga Web 2 (`icingaweb2` package). The `icinga2-classicui` package is still present to use the Icinga 1.x CGI web interface with Icinga 2, but the support for it will be removed in Icinga 2.11. Icinga Web 2 should be used instead.

- The Mailman mailing list manager suite version 3 is newly available 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 remains available in this release in the package `mailman`, so you can migrate any existing installations at your own pace. The Mailman 2.1 package will be kept in working order for the foreseeable future, but will not see any major changes or improvements. It will be removed from the first Debian release after Mailman upstream has stopped support for this branch.

  Everyone is encouraged to upgrade to Mailman 3, the modern release under active development.

- The packages `spf-milter-python` and `dkim-milter-python` are no longer actively developed upstream, but their more feature-rich replacements, `pyspf-milter` and `dkimpy-milter`, are available in buster. Users should migrate to the new packages before the old ones are removed in bullseye.

5.1.12   Ting at gøre efter opgradering og før genstart

When `apt full-upgrade` has finished, the "formal" upgrade is complete. For the upgrade to buster, there are no special actions needed before performing a reboot.

5.1.13   SysV init related packages no longer required

BEMÆRK

This section does not apply if you have decided to stick with sysvinit-core.

After the switch to systemd as default init system in Jessie and further refinements in Stretch, various SysV related packages are no longer required and can now be purged safely via

```
apt purge initscripts sysv-rc insserv startpar
```

5.2 Begrænsninger i sikkerhedsunderstøttelse

Der er nogle pakker hvor Debian ikke kan love at tilbyde minimale tilbageporteringer for sikkerheds-mæssige 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 Security status of web browsers and their rendering engines

Debian 10 includes several browser engines which are affected by a steady stream of security vulnera-bilities. 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 re-leases. Therefore, browsers built upon e.g. the webkit and khtml engines[1] are included in buster, but not covered by security support. These browsers should not be used against untrusted websites. The `webkit2gtk` source package is 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.

5.2.2 Go based packages

The Debian infrastructure currently doesn't properly enable rebuilding packages that statically link parts of other packages on a large scale. Until buster that hasn't been a problem in practice, but with the growth of the Go ecosystem it means that Go based packages won't be covered by regular security support until the infrastructure is improved to deal with them maintainably.

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

5.3 Pakkespecifikke problemstillinger

In most cases, packages should upgrade smoothly between stretch and buster. There are a small number of cases where some intervention may be required, either before or during the upgrade; these are detailed below on a per-package basis.

5.3.1 Semantics for using environment variables for su changed

`su` has changed semantics in buster and no longer preserves the user environment variables `DISPLAY` and `XAUTHORITY`. If you need to run graphical applications with `su`, you will have to explicitly set them to allow access to your display. See bug #905409 (`https://bugs.debian.org/905409`) for an extensive discussion.

5.3.2 Existing PostgreSQL databases need to be reindexed

When upgrading from stretch to buster, the `glibc` locale data is upgraded. Specifically, this changes how PostgreSQL sorts data in text indexes. To avoid corruption, such indexes need to be `REINDEX`ed immediately after upgrading the `locales` or `locales-all` packages, before putting the database back into production.

Suggested command:

---

[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`.

```
sudo -u postgres reindexdb --all
```

Alternatively, upgrade the databases to PostgreSQL 11 using **pg_upgradecluster**. (This uses **pg_dump** by default which will rebuild all indexes. Using `-m upgrade` or **pg_upgrade** is *not* safe because it preserves the now-wrong index ordering.)

Refer to the PostgreSQL Wiki (`https://wiki.postgresql.org/wiki/Locale_data_changes`) for more information.

5.3.3   mutt and neomutt

In stretch, the package `mutt` had patches applied from the sources at https://neomutt.org (`https://neomutt.org`). Starting from buster, the package providing `/usr/bin/mutt` will instead be purely based on the original sources from http://www.mutt.org (`http://www.mutt.org`), and a separate `neomutt` package is available providing `/usr/bin/neomutt`.

This means that some of the features that were previously provided by `mutt` are no longer available. If this breaks your configuration you can install `neomutt` instead.

5.3.4   Accessing GNOME Settings app without mouse

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

5.3.5   gnome-disk-utility fails to change LUKS password causing permanent data loss (buster 10.0 only)

Users of the initial buster release images should not change the LUKS password of encrypted disks with the GNOME graphical interface for disk management. The `gnome-disk-utility` package in buster had a very nasty bug (#928893) (`https://bugs.debian.org/928893`) when used to change the LUKS password: it deleted the old password but failed to correctly set the new one, making all data on the disk inaccessible. This has been fixed in the first point release.

5.3.6   evolution-ews has been dropped, and email inboxes using Exchange, Office365 or Outlook server will be removed

Users using `evolution` as their email client and connecting to a server running Exchange, Office365 or Outlook using the `evolution-ews` plugin should not upgrade to buster without backing up data and finding an alternative solution beforehand, as evolution-ews has been dropped due to bug #926712 (`https://bugs.debian.org/926712`) and their email inboxes, calendar, contact lists and tasks will be removed and will no longer be accessible with Evolution.

The `evolution-ews` package has been reintroduced via buster-backports. Users upgrading from stretch to buster can enable buster-backports after the upgrade and then they will be able to reinstall `evolution-ews`.

5.3.7   Calamares installer leaves disk encryption keys readable

When installing Debian from live media using the Calamares installer (Afsnit 2.2.13) and selecting the full disk encryption feature, the disk's unlock key is stored in the initramfs which is world readable. This allows users with local filesystem access to read the private key and gain access to the filesystem again in the future.

This can be worked around by adding `UMASK=0077` to `/etc/initramfs-tools/conf.d/initramfs-permission` and running **update-initramfs -u**. This will recreate the initramfs without world-readable permissions.

A fix for the installer is being planned (see bug #931373 (`https://bugs.debian.org/931373`)) and will be uploaded to debian-security. In the meantime users of full disk encryption should apply the above workaround.

5.3.8   S3QL URL changes for Amazon S3 buckets

When using `s3ql` with Amazon S3 buckets, the configuration needs updating for a change in the URL. The new format is:

```
s3://<region>/<bucket>/<prefix>
```

5.3.9   Split in configuration for logrotate

The shipped configurations for `/var/log/btmp` and `/var/log/wtmp` have been split from the main configuration file (`/etc/logrotate.conf`) into separate standalone files (`/etc/logrotate.d/btmp` and `/etc/logrotate.d/wtmp`).

If you have modified `/etc/logrotate.conf` in this regard, make sure to re-adjust the two new files to your needs and drop any references to (b|w)tmp from the main file, since duplicate definitions can cause errors.

5.3.10   The **rescue** boot option is unusable without a root password

With the implementation of `sulogin` now used, 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/buster//buster/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/buster//buster/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`).

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 stretch-system før opgraderingen

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

A.1 Opgradering af dit stretch-system

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

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/buster//buster/apt/sources.list.5.html`)) contain references to "`stable`", this is effectively pointing to buster 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 buster, er der ikke længere meget mening i at installere pakker fra stretch. 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 `stretch`.

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 stretch or buster 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 buster, så anbefales det at fjerne gamle konfigurationsfiler (såsom `*.dpkg-{new,old}`-filer under `/etc` fra systemet.

A.4 Opgrader forældede sprogindstillinger til UTF-8

Using a legacy non-UTF-8 locale has been unsupported by desktops and other mainstream software projects for a long time. Such locales should be upgraded by running **dpkg-reconfigure locales** and selecting a UTF-8 default. You should also ensure that users are not overriding the default to use a legacy locale in their environment.

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