

# **Hinweise zur Debian-Veröffentlichung Version 10 (Buster) auf ARM 64-Bit**

Das Debian-Dokumentationsprojekt (<https://www.debian.org/doc/>)

4. Juli 2022

---

## Hinweise zur Debian-Veröffentlichung Version 10 (Buster) auf ARM 64-Bit

Dieses Dokument ist freie Software. Sie können es unter den Bedingungen der GNU General Public License Version 2, wie von der Free Software Foundation herausgegeben, weitergeben und/oder modifizieren.

Die Veröffentlichung dieses Dokuments erfolgt in der Hoffnung, dass es Ihnen von Nutzen sein wird, aber OHNE JEDE GEWÄHRLEISTUNG - sogar ohne die implizite Gewährleistung der MARKTREIFE oder der EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. Details finden Sie in der GNU General Public License.

Sie sollten eine Kopie der GNU General Public License zusammen mit diesem Dokument erhalten haben. Falls nicht, schreiben Sie an die Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Den Lizenztext finden Sie außerdem unter <https://www.gnu.org/licenses/gpl-2.0.html> und in `/usr/share/common-licenses/GPL-2` auf jedem Debian-System.

# Inhaltsverzeichnis

<b>1</b>	<b>Einführung</b>	<b>1</b>
1.1	Fehler in diesem Dokument berichten	1
1.2	Upgrade-Berichte zur Verfügung stellen	1
1.3	Quelltext dieses Dokuments	2
<b>2</b>	<b>Was ist neu in Debian 10</b>	<b>3</b>
2.1	Unterstützte Architekturen	3
2.2	Was ist neu in der Distribution?	3
2.2.1	UEFI Secure Boot	4
2.2.2	AppArmor standardmäßig aktiviert	5
2.2.3	Optionales Härten von APT	5
2.2.4	unattended-upgrades für Stable-Zwischenveröffentlichungen	5
2.2.5	Wesentlich verbesserte Handbuchseiten für Deutsch-sprechende Nutzer	5
2.2.6	Filterung des Netzwerk-Verkehrs standardmäßig basierend auf nftables	5
2.2.7	Cryptsetup setzt standardmäßig auf das on-disk LUKS2-Format	6
2.2.8	Driverless printing with CUPS 2.2.10	6
2.2.9	Basisunterstützung für Allwinner-A64-basierte Geräte	7
2.2.10	News from Debian Med Blend	7
2.2.11	GNOME defaults to Wayland	7
2.2.12	Merged /usr on fresh installs	7
2.2.13	News from Debian Live team	8
<b>3</b>	<b>Installationssystem</b>	<b>9</b>
3.1	Was ist neu im Installationssystem?	9
3.1.1	Automatisierte Installation	9
<b>4</b>	<b>Upgrade von Debian 9 (Stretch)</b>	<b>11</b>
4.1	Vorbereiten des Upgrades	11
4.1.1	Sichern aller Daten und Konfigurationsinformationen	11
4.1.2	Die Benutzer vorab informieren	11
4.1.3	Vorbereitung auf die Deaktivierung von Diensten	12
4.1.4	Vorbereitungen für eine Systemwiederherstellung	12
4.1.4.1	Shell zur Fehleranalyse während des Bootens mit Initrd	12
4.1.4.2	Shell zur Fehleranalyse während des Bootens mit systemd	13
4.1.5	Vorbereiten einer sicheren Umgebung für das Upgrade	13
4.1.6	Kontrolle der Netzwerkschnittstellen-Bezeichnungen	13
4.2	Status der APT-Konfiguration überprüfen	13
4.2.1	Der Bereich für vorgeschlagene Aktualisierungen („proposed-updates“)	14
4.2.2	Inoffizielle Quellen	14
4.2.3	APT Pinning deaktivieren	14
4.2.4	Paketstatus überprüfen	14
4.3	Die APT source-list-Dateien vorbereiten	15
4.3.1	APT-Internet-Quellen hinzufügen	16
4.3.2	APT-Quellen für einen lokalen Spiegel hinzufügen	16
4.3.3	APT-Quellen für optische Medien hinzufügen	17
4.4	Upgrades von Paketen durchführen	17
4.4.1	Aufzeichnung der Sitzung	18
4.4.2	Aktualisieren der Paketliste	18
4.4.3	Sicherstellen, dass genügend Speicherplatz für das Upgrade zur Verfügung steht	18
4.4.4	Minimales System-Upgrade	21
4.4.5	Upgrade des Systems	21
4.5	Mögliche Probleme während des Upgrades	21
4.5.1	dist-upgrade schlägt fehl mit „Could not perform immediate configuration“	21
4.5.2	Zu erwartende Paketentfernungen	22

4.5.3	Conflicts- oder Pre-Depends-Schleifen	22
4.5.4	Dateikonflikte	22
4.5.5	Konfigurationsänderungen	23
4.5.6	Ändern der aktuellen Sitzung auf die Konsole	23
4.6	Upgrade des Kernels und zugehöriger Pakete	23
4.6.1	Ein Kernel-Metapaket installieren	23
4.7	Vorbereiten auf die nächste Veröffentlichung	24
4.7.1	Vollständiges Löschen entfernter Pakete	24
4.8	Veraltete Pakete	25
4.8.1	Übergangs-Dummy-Pakete	25
<b>5</b>	<b>Dinge, die Sie über Buster wissen sollten</b>	<b>27</b>
5.1	Upgrade-spezifische Themen für Buster	27
5.1.1	Mount-Option <code>hidepid</code> für <code>procs</code> nicht mehr unterstützt	27
5.1.2	Start von <code>ybind</code> mit <code>-no-dbus</code> schlägt fehl	27
5.1.3	NIS server does not answer NIS client requests by default	27
5.1.4	Authentifizierung von <code>sshd</code> schlägt fehl	27
5.1.5	Daemon-Prozesse starten nicht mehr oder das System scheint während des Boot-Vorgangs zu hängen	28
5.1.6	Migration von altbekannten Netzwerkschnittstellen-Namen	28
5.1.7	Module configuration for bonding and dummy interfaces	29
5.1.8	OpenSSL-Standard-Version und erhöhtes Sicherheits-Level	29
5.1.9	Einige Anwendungen funktionieren nicht in GNOME mit Wayland	30
5.1.10	Nennenswerte veraltete Pakete	30
5.1.11	Missbilligte Komponenten für Buster	30
5.1.12	Dinge, die vor dem Neustart erledigt werden sollten	31
5.1.13	SysV-init betreffende Pakete nicht länger benötigt	31
5.2	Einschränkungen bei der Sicherheitsunterstützung	31
5.2.1	Sicherheitsstatus von Webbrowsern und deren Rendering-Engines	31
5.2.2	Go based packages	32
5.3	Eingriffe bei einigen spezifischen Paketen	32
5.3.1	Semantik für die Nutzung von Umgebungsvariablen durch <code>su</code> geändert	32
5.3.2	Neuindexierung vorhandener PostgreSQL-Datenbanken erforderlich	32
5.3.3	<code>mutt</code> und <code>neomutt</code>	32
5.3.4	Accessing GNOME Settings app without mouse	33
5.3.5	<code>gnome-disk-utility</code> fails to change LUKS password causing permanent data loss (buster 10.0 only)	33
5.3.6	<code>evolution-ews</code> has been dropped, and email inboxes using Exchange, Office365 or Outlook server will be removed	33
5.3.7	<code>Calamares</code> installer leaves disk encryption keys readable	33
5.3.8	S3QL URL changes for Amazon S3 buckets	33
5.3.9	Split in configuration for <code>logrotate</code>	34
5.3.10	The <code>rescue</code> boot option is unusable without a root password	34
<b>6</b>	<b>Zusätzliche Informationen zu Debian</b>	<b>35</b>
6.1	Weitere Lektüre	35
6.2	Hilfe bekommen	35
6.2.1	Mailinglisten	35
6.2.2	Internet Relay Chat	35
6.3	Fehler berichten	35
6.4	Zu Debian beitragen	36
<b>7</b>	<b>Glossar</b>	<b>37</b>
<b>A</b>	<b>Verwalten Ihres Stretch-Systems vor dem Upgrade</b>	<b>39</b>
A.1	Upgrade Ihres Stretch-Systems	39
A.2	Überprüfen Ihrer Paketquellen (APT source-list-Dateien)	39
A.3	Veraltete Konfigurationsdateien entfernen	40
A.4	Upgrade von veralteten Gebietsschemata (Locales) auf UTF-8	40

<b>B Mitwirkende bei den Veröffentlichungshinweisen</b>	<b>41</b>
<b>Index</b>	<b>43</b>



# Kapitel 1

## Einführung

Dieses Dokument informiert Benutzer der Debian-Distribution über entscheidende Änderungen in Version 10 (Codename Buster).

Die Hinweise zur Veröffentlichung enthalten Informationen, wie ein sicheres Upgrade von Version 9 (Codename Stretch) auf die aktuelle Veröffentlichung durchgeführt werden kann und informieren die Benutzer über bekannte potenzielle Probleme, die während des Upgrades auftreten können.

Die neueste Version dieses Dokuments erhalten Sie unter <https://www.debian.org/releases/buster/releasenotes>. Im Zweifelsfall prüfen Sie das Datum auf der ersten Seite, um sich zu vergewissern, dass Sie eine aktuelle Version lesen.

### ACHTUNG



Beachten Sie, dass es unmöglich ist, alle bekannten Probleme aufzulisten; deshalb wurde eine Auswahl getroffen, basierend auf einer Kombination aus der zu erwartenden Häufigkeit des Auftretens und der Auswirkung der Probleme.

Bitte gestatten Sie uns die Anmerkung, dass wir lediglich ein Upgrade von der letzten Version (in diesem Fall Stretch) auf die aktuelle unterstützen können. Falls Sie ein Upgrade von einer noch älteren Version durchführen müssen, empfehlen wir dringend, dass Sie die früheren Ausgaben der Veröffentlichungshinweise lesen und zuerst ein Upgrade auf Stretch durchführen.

### 1.1 Fehler in diesem Dokument berichten

Wir haben versucht, die einzelnen Schritte des Upgrades in diesem Dokument zu beschreiben und alle möglicherweise auftretenden Probleme vorherzusehen.

Falls Sie dennoch einen Fehler in diesem Dokument gefunden haben (fehlerhafte oder fehlende Informationen), senden Sie bitte einen entsprechenden Fehlerbericht über das Paket `release-notes` an unsere [Fehlerdatenbank](https://bugs.debian.org/) (<https://bugs.debian.org/>). Sie können auch zunächst die [bereits vorhandenen Fehlerberichte](https://bugs.debian.org/release-notes) (<https://bugs.debian.org/release-notes>) lesen für den Fall, dass das Problem, welches Sie gefunden haben, schon berichtet wurde. Sie dürfen gerne zusätzliche Informationen zu solchen bereits vorhandenen Fehlerberichten hinzufügen, wenn Sie Inhalte zu diesem Dokument beitragen können.

Wir begrüßen Fehlerberichte, die Patches für den Quellcode des Dokuments bereitstellen und möchten Sie sogar dazu ermuntern, solche einzureichen. Mehr Informationen darüber, wie Sie den Quellcode bekommen, finden Sie in Abschnitt [1.3](#).

### 1.2 Upgrade-Berichte zur Verfügung stellen

Wir begrüßen jede Information von unseren Benutzern, die sich auf ein Upgrade von Stretch auf Buster bezieht. Falls Sie solche Informationen bereitstellen möchten, senden Sie bitte einen Fehlerbericht

mit den entsprechenden Informationen gegen das Paket `upgrade-reports` an unsere **Fehlerdatenbank** (<https://bugs.debian.org/>). Wir bitten Sie, alle Anhänge, die Sie Ihrem Bericht beifügen, zu komprimieren (mit dem Befehl **gzip**).

Bitte fügen Sie Ihrem Upgrade-Bericht folgende Informationen bei:

- Den Status Ihrer Paketdatenbank vor und nach dem Upgrade: Die Statusdatenbank von `dpkg` finden Sie unter `/var/lib/dpkg/status`, die Paketstatusinformationen von `apt` unter `/var/lib/apt/extended_states`. Sie sollten vor dem Upgrade eine Sicherung dieser Daten erstellen (wie unter Abschnitt 4.1.1 beschrieben). Sicherungen von `/var/lib/dpkg/status` sind aber auch in `/var/backups` zu finden.
- Upgrade-Protokolle, erstellt mit Hilfe des Befehls **script** (wie in Abschnitt 4.4.1 beschrieben).
- Ihre `apt`-Logdateien, die Sie unter `/var/log/apt/term.log` finden, oder Ihre **aptitude**-Logdateien, die unter `/var/log/aptitude` zu finden sind.

#### ANMERKUNG



Sie sollten sich ein wenig Zeit nehmen, um die Informationen zu prüfen und sensible bzw. vertrauliche Daten aus den Logdateien zu löschen, bevor Sie die Informationen dem Fehlerbericht anhängen, da der gesamte Bericht mit Ihren Anhängen öffentlich gespeichert und einsehbar sein wird.

## 1.3 Quelltext dieses Dokuments

Die Quellen für dieses Dokument liegen im DocBook-XML-Format vor. Die HTML-Version wird mit `docbook-xsl` und `xsltproc` erstellt. Die PDF-Version wird mit `dblatex` oder `xmlroff` erstellt. Die Quellen der Veröffentlichungshinweise sind im GIT-Depot des *Debian-Dokumentationsprojekts* verfügbar. Sie können die **Web-Oberfläche** (<https://salsa.debian.org/ddp-team/release-notes/>) nutzen, um die einzelnen Dateien und ihre Änderungen einzusehen. Für weitere Informationen zum Umgang mit GIT beachten Sie bitte die **GIT-Informationsseiten** (<https://www.debian.org/doc/vcs>) des Debian-Dokumentationsprojekts.



# Kapitel 2

## Was ist neu in Debian 10

Das [Wiki](https://wiki.debian.org/NewInBuster) (<https://wiki.debian.org/NewInBuster>) enthält weitere Informationen zu diesem Thema.

### 2.1 Unterstützte Architekturen

Die folgenden Architekturen werden offiziell von Debian 10 unterstützt:

- 32-Bit PC (`i386`) und 64-Bit PC (`amd64`)
- 64-Bit ARM (`arm64`)
- ARM EABI (`armel`)
- ARMv7 (EABI Hard-Float ABI, `armhf`)
- MIPS (`mips` (Big-Endian) und `mipsel` (Little-Endian))
- 64-Bit Little-Endian MIPS (`mips64el`)
- 64-Bit Little-Endian PowerPC (`ppc64el`)
- IBM System z (`s390x`)

Näheres zum Stand der Portierungen und Port-spezifische Informationen für Ihre Architektur finden Sie auf [Debian's Portierungs-Webseiten](https://www.debian.org/ports/) (<https://www.debian.org/ports/>).

### 2.2 Was ist neu in der Distribution?

Diese neue Version von Debian erscheint wieder mit erheblich mehr Software als ihr Vorgänger Stretch; die Distribution enthält über 13370 neue Pakete und damit insgesamt über 57703 Pakete. Ein Großteil der Software in der Distribution wurde aktualisiert: über 35532 Softwarepakete (das entspricht 62% aller Pakete in Stretch). Außerdem wurde eine signifikante Zahl von Paketen (über 7278, 13% der Pakete in Stretch) aus verschiedenen Gründen aus der Distribution entfernt. Für diese Pakete werden Sie keine Aktualisierungen finden und sie werden in den Paketverwaltungsprogrammen als „veraltet“ (obsolete) markiert sein; lesen Sie dazu auch Abschnitt [4.8](#).

Debian erscheint wieder mit verschiedenen Desktop-Anwendungen und -Umgebungen. Unter anderem enthält es die Desktop-Umgebungen GNOME 3.30, KDE Plasma 5.14, LXDE 10, LXQt 0.14, MATE 1.20 und Xfce 4.12.

Produktivprogramme wurden ebenfalls aktualisiert, inklusive der Büroanwendungs-Pakete:

- LibreOffice wurde auf Version 6.1 aktualisiert;
- Calligra wurde auf Version 3.1 aktualisiert.
- GnuCash wurde auf Version 3.4 aktualisiert;

Mit der Buster-Veröffentlichung enthält Debian erstmals ein standardmäßig aktiviertes System für „Mandatory Access Control“ (in Deutsch etwa: zwingend erforderliche Zugangskontrolle). Neue Installationen von Debian Buster haben AppArmor installiert und aktiviert. Weitere Informationen finden Sie weiter unten.

Außerdem ist Buster die erste Debian-Veröffentlichung, die Rust-basierte Programme wie Firefox, ripgrep, fd, exa usw. mitbringt sowie eine signifikante Anzahl Rust-basierter Bibliotheken (mehr als 450). Buster enthält Rustc 1.34.

Zu weiteren Aktualisierungen von Desktop-Anwendungen gehört auch das Upgrade auf Evolution 3.30.

Neben vielen weiteren enthält diese Veröffentlichung auch folgende Aktualisierungen:

Paket	Version in 9 (Stretch)	Version in 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 und 25.1	26.1
Exim - Standard-E-Mail-Server	4.89	4.92
GNU Compiler Collection als Standard-Kompiliersoftware	6.3	7.4 und 8.3
GIMP	2.8.18	2.10.8
GnuPG	2.1	2.2
Inkscape	0.92.1	0.92.4
GNU-C-Bibliothek	2.24	2.28
lighttpd	1.4.45	1.4.53
Linux-Kernel-Image	4.9-Serie	4.19-Serie
LLVM/Clang-Werkzeugkette	3.7	6.0.1 und 7.0.1 (Standardversion)
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 ist eine Funktionalität, die auf den meisten aktuellen PCs aktiviert ist und verhindert, dass beim Booten unsignierter Code geladen wird. Dies soll vor einigen Arten von Bootkits und Rootkits schützen.

Debian kann jetzt auf den meisten PCs, auf denen Secure Boot aktiviert ist, installiert werden.

Es ist möglich, Secure Boot auf Systemen zu aktivieren, auf denen bereits eine Debian-Installation vorhanden ist, sofern das System mittels UEFI bootet. Zuvor ist es aber erforderlich, `shim-signed`, `grub-efi-amd64-signed` oder `grub-efi-ia32-signed` zu installieren sowie ein Linux-Kernel-Paket aus Debian Buster.

Einige Funktionen von GRUB und Linux sind im Secure-Boot-Modus eingeschränkt, um Modifikationen an deren Code zu verhindern.

Weitere Informationen finden Sie Im Debian Wiki unter [SecureBoot](https://wiki.debian.org/SecureBoot) (<https://wiki.debian.org/SecureBoot>).

### 2.2.2 AppArmor standardmäßig aktiviert

In Debian Buster ist AppArmor standardmäßig aktiviert. AppArmor ist ein System für „Mandatory Access Control“ (in Deutsch etwa: zwingend erforderliche Zugangskontrolle). Dieses ordnet verschiedenen Anwendungen über entsprechende Profile speziell zugeschnittene Berechtigungen zu, wie Berechtigungen für mount, ptrace und das Senden von Systemsignalen oder Lese-, Schreib- und Ausführungsrechte für Dateien.

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 Optionales Härten von APT

Alle von APT bereitgestellten Methoden (z.B. `http` und `https`) außer `cdrom`, `gpgv` und `rsh` können das vom Linux-Kernel angebotene `seccomp-BPF-Sandboxing` verwenden, um die dabei erlaubten Systemaufrufe einzuschränken; alle anderen Aufrufe werden dabei mittels `SIGSYS`-Signalen abgefangen. Das Sandboxing ist derzeit optional und muss bewußt aktiviert werden über:

```
APT::Sandbox::Seccomp ist ein bool'scher Wert, um die Funktionalitäten
ein- oder auszuschalten.
```

Es gibt zwei Optionen, mit denen die Funktionalität detaillierter konfiguriert werden kann:

```
APT::Sandbox::Seccomp::Trap ist eine Liste weiterer Systemaufrufe, die
abgefangen werden sollen.
APT::Sandbox::Seccomp::Allow ist eine Liste weiterer Systemaufrufe, die
erlaubt sein sollen.
```

### 2.2.4 unattended-upgrades für Stable-Zwischenveröffentlichungen

Frühere Versionen von `unattended-upgrades` waren standardmäßig so eingestellt, dass sie nur Upgrades installiert haben, die von der Security-Suite bereitgestellt wurden. In Buster wird jetzt das System auch automatisch auf die neueste Zwischenveröffentlichung aktualisiert. Details hierzu finden Sie in der `NEWS.Debian`-Datei des Pakets.

### 2.2.5 Wesentlich verbesserte Handbuchseiten für Deutsch-sprechende Nutzer

Die Programmdokumentation (`manpages` oder Handbuchseiten) für verschiedene Software wie `systemd`, `util-linux` und `mutt` wurde für Deutsch beträchtlich erweitert. Bitte installieren Sie das Paket `manpages-de`, um von diesen Verbesserungen zu profitieren. Während des Lebenszyklus von Debian Buster werden weitere neue/verbesserte Übersetzungen über das `backports`-Archiv bereitgestellt.

### 2.2.6 Filterung des Netzwerk-Verkehrs standardmäßig basierend auf nftables

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.

Dies gilt für alle dazugehörigen Programme und Werkzeuge:

- `iptables`
- `iptables-save`
- `iptables-restore`

- iptables
- iptables-save
- iptables-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 encouraged to switch to the `nftables` interface rather than using `iptables`.

`nftables` bietet einen vollwertigen Ersatz für `iptables`, aber mit erheblich besserer Performance, einer aufgefrischten Syntax, besserer Unterstützung für IPv4/IPv6 Dual-Stack-Firewalls, vollständig autonomen Operationen für dynamische Aktualisierungen der Regelsätze, eine Netlink-API für Dritt-Anbieter-Anwendungen, schnellere Paketklassifizierung durch verbesserte generische `set`- und `map`-Infrastrukturen, sowie **vielen anderen Verbesserungen** (<https://wiki.nftables.org>).

Diese Änderung ist konform mit dem, was andere große Linux-Distributionen wie RedHat tun, die jetzt `nftables` als **Standard-Firewall-Werkzeug** ([https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/8-beta/html-single/8.0\\_beta\\_release\\_notes/index#networking\\_2](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8-beta/html-single/8.0_beta_release_notes/index#networking_2)) einsetzen.

Beachten Sie auch, dass alle `iptables`-Binärdateien jetzt in `/usr/sbin` installiert sind (statt wie früher in `/sbin`). Ein symbolischer Link ist zu Kompatibilitätszwecken vorhanden, wird aber nach dem Lebenszyklus von Debian Buster entfernt werden. Hart-codierte Binärpfade in Skripten müssen aktualisiert werden und sollten daher vermieden werden.

Ausführliche Dokumentation finden Sie in den README- und NEWS-Dateien des Pakets sowie im **Debian Wiki** (<https://wiki.debian.org/nftables>).

### 2.2.7 Cryptsetup setzt standardmäßig auf das on-disk LUKS2-Format

Die `cryptsetup`-Version in Debian Buster setzt standardmäßig auf das neue on-disk LUKS2-Format. Neue LUKS-Volumes werden per Voreinstellung dieses Format benutzen.

Anders als das vorherige LUKS1-Format bietet LUKS2 Redundanz der Metadaten, Erkennung korrupter Metadaten und konfigurierbare PBKDF-Algorithmen. Authentifizierte Verschlüsselung wird ebenfalls unterstützt, ist jedoch noch experimentell.

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 bringt CUPS 2.2.10 mit sowie `cups-filters` 1.21.6. Zusammen bieten sie dem Nutzer alles, was nötig ist, um von den Vorzügen von **treiberlosem Drucken (driverless printing)** (<https://wiki.debian.org/DriverlessPrinting>) profitieren zu können. Dafür ist grundsätzlich erforderlich, dass eine Netzwerk-Druckerwarteschlange oder ein Drucker den AirPrint-Service bereitstellt. Ein moderner IPP-Drucker ist mit hoher Wahrscheinlichkeit AirPrint-fähig; auch eine Druckerwarteschlange aus Debian CUPS ist AirPrint-fähig.

Im Wesentlichen können die DNS-SD-Broadcasts (Bonjour) eines CUPS-Servers, der eine Druckerwarteschlange anbietet, oder eines IPP-Druckers ohne Zutun des Nutzers in dem Druckdialog der Anwendungen angezeigt werden. Als zusätzlichem Nutzen kann auf diesem Wege auf nicht-freie Druckertreiber der Hardware-Hersteller verzichtet werden.

Eine Standardinstallation des cups-Pakets installiert auch das Paket cups-browsed; Druckerwarteschlangen und IPP-Drucker werden jetzt automatisch von diesem Hilfsprogramm eingerichtet und verwaltet. Dies ist der empfohlene Weg, um dem Nutzer ein nahtloses und störungsfreies Drucken über das neue treiberlose System bieten zu können; siehe dazu den [Beitrag im Debian-Wiki \(englisch\)](https://wiki.debian.org/QuickPrintQueuesCUPS) (<https://wiki.debian.org/QuickPrintQueuesCUPS>).

## 2.2.9 Basisunterstützung für Allwinner-A64-basierte Geräte

Thanks to the efforts of the [linux-sunxi community](https://linux-sunxi.org) (<https://linux-sunxi.org>) Debian buster will have basic support 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) (<https://backports.debian.org>). See also [the status page](https://linux-sunxi.org/Linux_mainlining_effort) ([https://linux-sunxi.org/Linux\\_mainlining\\_effort](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) (<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 Abschnitt [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 → /usr/bin
/sbin → /usr/sbin
/lib → /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) (<https://www.freedesktop.org>) project hosts a [Wiki](https://www.freedesktop.org/wiki/Software/systemd/TheCaseForTheUsrMerge/) (<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

## Installationssystem

Der Debian-Installer ist das offizielle Installationssystem für Debian. Er bietet verschiedene Installationsmethoden an. Welche dieser Methoden für Ihr System zur Verfügung stehen, hängt von der verwendeten Architektur ab.

Images des Installers für Buster finden Sie zusammen mit der Installationsanleitung auf der [Debian-Webseite](https://www.debian.org/releases/buster/debian-installer/) (<https://www.debian.org/releases/buster/debian-installer/>).

Die Installationsanleitung ist ebenfalls dem ersten Medium des offiziellen Debian-DVD/CD/Blu-Ray-Satzes beigelegt unter:

```
/doc/install/manual/language/index.html
```

Beachten Sie bitte auch die [Errata](https://www.debian.org/releases/buster/debian-installer/index#errata) (<https://www.debian.org/releases/buster/debian-installer/index#errata>) für den Debian-Installer bezüglich bekannter möglicher Probleme.

### 3.1 Was ist neu im Installationssystem?

Am Debian-Installer wurde seit seiner letzten offiziellen Veröffentlichung in Debian 9 viel entwickelt, was zu verbesserter Hardware-Unterstützung sowie einigen spannenden neuen Funktionen oder Verbesserungen führt.

Erwähnenswert ist hier die initiale Unterstützung für UEFI Secure Boot (siehe Abschnitt [2.2.1](#)), die zu den Installations-Images hinzugefügt wurde.

Falls Sie an einem detaillierten Überblick über die Änderungen seit Stretch interessiert sind, beachten Sie bitte die Ankündigungen (Release Announcements) für die Buster Beta- und RC-Veröffentlichungen unter [Letzte Neuigkeiten zum Debian-Installer](https://www.debian.org/devel/debian-installer/News/) (<https://www.debian.org/devel/debian-installer/News/>).

#### 3.1.1 Automatisierte Installation

Viele der bisher genannten Änderungen ziehen auch Änderungen für die Funktionalität des Installers nach sich, automatisierte Installationen mit Hilfe von Vorkonfigurationsdateien durchzuführen. Das bedeutet, Sie können nicht davon ausgehen, dass alte Vorkonfigurationsdateien, die mit Stretch funktioniert haben, nun auch mit dem neuen Installer funktionieren, zumindest nicht ohne Anpassungen.

Die [Installationsanleitung](https://www.debian.org/releases/buster/installmanual) (<https://www.debian.org/releases/buster/installmanual>) enthält einen aktualisierten Anhang mit ausführlicher Dokumentation über die Verwendung der Vorkonfiguration.





# Kapitel 4

## Upgrade von Debian 9 (Stretch)

### 4.1 Vorbereiten des Upgrades

Wir empfehlen, dass Sie vor dem Upgrade auch die Informationen in Kapitel 5 lesen. Das Kapitel behandelt mögliche Probleme, die mit dem Upgrade-Prozess nicht direkt zusammenhängen, von denen Sie aber dennoch wissen sollten, bevor Sie mit dem Upgrade beginnen.

#### 4.1.1 Sichern aller Daten und Konfigurationsinformationen

Wir empfehlen Ihnen nachdrücklich, vor dem Upgrade Ihres Systems ein komplettes Backup durchzuführen oder zumindest alle Daten und Konfigurationsinformationen zu sichern, die Sie nicht verlieren möchten. Die Upgrade-Werkzeuge und der zugehörige Prozess sind recht zuverlässig, aber ein Versagen der Hardware während des Upgrades könnte zu einem schwer beschädigten System führen.

Am wichtigsten für das Backup sind die Inhalte von `/etc`, `/var/lib/dpkg`, `/var/lib/apt/extended_states` und die Ausgabe von `dpkg --get-selections "*" (die Anführungszeichen sind wichtig)`. Falls Sie **aptitude** verwenden, um die Pakete auf Ihrem System zu verwalten, sollten Sie auch `/var/lib/aptitude/pkgstates` sichern.

Der Upgrade-Prozess ändert nichts im Verzeichnisbaum `/home`. Allerdings ist bekannt, dass einige Anwendungen (z.B. Teile der Mozilla-Suite und die GNOME- und KDE-Desktop-Umgebungen) existierende Benutzereinstellungen mit neuen Vorgaben überschreiben, wenn eine neue Version der Anwendung das erste Mal von einem Benutzer gestartet wird. Zur Vorsicht sollten Sie überlegen, die versteckten Dateien und Verzeichnisse (Dateien und Verzeichnisse, die mit einem Punkt beginnen, auch „dotfiles“ genannt) in den Home-Verzeichnissen der Benutzer zu sichern. Dieses Backup könnte Ihnen dabei helfen, die alten Einstellungen wiederherzustellen. Auch sollten Sie die Benutzer des Systems darüber informieren.

Jede Paketinstallation muss mit den Rechten des Superusers ausgeführt werden. Melden Sie sich daher als `root` an oder verwenden Sie **su** oder **sudo**, um die notwendigen Rechte zu erlangen.

Für das Upgrade gibt es ein paar Voraussetzungen; Sie sollten diese überprüfen, bevor Sie das Upgrade durchführen.

#### 4.1.2 Die Benutzer vorab informieren

Es empfiehlt sich, alle Benutzer vor dem geplanten Upgrade zu informieren, auch wenn Benutzer, die über **ssh** auf Ihr System zugreifen, wenig von dem Upgrade mitbekommen sollten und es ihnen möglich sein sollte, weiterzuarbeiten.

Falls Sie zusätzliche Vorsichtsmaßnahmen ergreifen möchten, sichern Sie die Partition `/home` vor dem Upgrade oder lösen Sie diese Einbindung mit **umount**.

Sie müssen beim Upgrade auf Buster auch ein Kernel-Upgrade durchführen, daher wird ein Systemneustart notwendig sein. Typischerweise wird dieser stattfinden, nachdem das Upgrade abgeschlossen ist.

### 4.1.3 Vorbereitung auf die Deaktivierung von Diensten

Einigen Paketen, für die ein Upgrade ansteht, sind möglicherweise Dienste zugeordnet. Falls das der Fall ist, beachten Sie bitte, dass diese Dienste während des Upgrades gestoppt werden, wenn die ihnen zugeordneten Pakete ersetzt und konfiguriert werden. Während dieser Zeit werden diese Dienste nicht verfügbar sein.

Die exakte Dauer, für die die Dienste abgeschaltet sind, variiert abhängig von der Anzahl der Pakete, die im System aktualisiert werden und enthält auch die Zeit, die der Systemadministrator benötigt, um Konfigurationsfragen von verschiedenen Paket-Upgrades zu beantworten. Beachten Sie, dass eine hohe Wahrscheinlichkeit für die Nichtverfügbarkeit von Diensten über eine erhebliche Zeitdauer besteht, wenn der Upgrade-Prozess unbeaufsichtigt läuft und das System eine Bedieneingabe während des Prozesses erfordert<sup>1</sup>.

Wenn das zu aktualisierende System kritische Dienste für Ihre Nutzer oder für das Netzwerk bereitstellt<sup>2</sup>, können Sie die Dauer, für die der Dienst abgeschaltet ist, reduzieren, indem Sie ein minimales System-Upgrade durchführen (wie in Abschnitt 4.4.4 beschrieben), gefolgt von einem Kernel-Upgrade und einem Reboot und schließlich dem Upgrade der Pakete, denen Ihre kritischen Dienste zugeordnet sind. Aktualisieren Sie diese Pakete, bevor Sie das eigentliche vollständige Upgrade durchführen, das in Abschnitt 4.4.5 beschrieben ist. So stellen Sie sicher, dass die kritischen Dienste während des ganzen vollständigen Upgrades laufen und verfügbar sind, so dass der Zeitraum, während dem die Dienste abgeschaltet sind, insgesamt reduziert ist.

### 4.1.4 Vorbereitungen für eine Systemwiederherstellung

Obwohl Debian versucht sicherzustellen, dass Ihr System immer startfähig bleibt, gibt es stets die Möglichkeit, dass Sie beim Neustart des Systems nach dem Upgrade Probleme feststellen. Bekannte mögliche Probleme sind in diesem und den nächsten Kapiteln dieser Veröffentlichungshinweise dokumentiert.

Aus diesem Grund ist es sinnvoll, sicherzustellen, dass Sie die Möglichkeit haben, Ihr System wieder zum Laufen zu bringen, falls der Start fehlschlagen sollte oder (bei fernverwalteten Systemen) der Aufbau der Netzwerkverbindung nicht erfolgreich sein sollte.

Falls Sie das Upgrade aus der Ferne über eine `ssh`-Verbindung durchführen, wird empfohlen, dass Sie die nötigen Vorkehrungen treffen, um den Server über eine serielle Terminalverbindung aus der Ferne erreichen zu können. Es besteht die Möglichkeit, dass Sie nach dem Kernel-Upgrade und anschließenden Neustart die Systemkonfiguration über eine lokale Konsole korrigieren müssen. Auch könnte es sein, dass Sie das System über eine lokale Konsole wiederherstellen müssen, wenn es in der Mitte des Upgrade-Prozesses versehentlich neu gebootet wird.

Zur Systemrettung oder Behebung von Problemen empfehlen wir normalerweise die Verwendung vom *Rettungsmodus* des Debian-Installers für Buster. Der Vorteil der Verwendung des Installers besteht darin, dass Sie aus seinen vielen Methoden diejenige aussuchen können, die am besten für Sie passt. Für weitere Informationen lesen Sie bitte den Abschnitt „Ein beschädigtes System reparieren“ in Kapitel 8 der [Installationsanleitung](https://www.debian.org/releases/buster/installmanual) (<https://www.debian.org/releases/buster/installmanual>) und die [FAQ des Debian-Installers](https://wiki.debian.org/DebianInstaller/FAQ) (<https://wiki.debian.org/DebianInstaller/FAQ>).

Falls dies fehlschlägt, benötigen Sie eine alternative Möglichkeit, Ihr System zu starten und zu reparieren. Eine Möglichkeit ist, ein spezielles Rettungs-Image oder eine Linux-Live-CD zu verwenden. Nachdem Sie davon gebootet haben, sollten Sie die Wurzel Ihres Dateisystems (`/`) einbinden und ein `chroot` darauf ausführen, um das Problem zu untersuchen und zu beheben.

#### 4.1.4.1 Shell zur Fehleranalyse während des Bootens mit `initrd`

Das `initramfs-tools`-Paket integriert eine Shell zur Fehleranalyse<sup>3</sup> in die `initrds`, die es erzeugt. Falls die `initrd` beispielsweise nicht in der Lage ist, die Wurzel Ihres Dateisystems (`/`) einzubinden, wird Ihnen diese Debug-Shell präsentiert, in der die grundlegenden Befehle vorhanden sind, um das Problem zu ermitteln und möglicherweise zu beheben.

---

<sup>1</sup>Wenn die `debconf`-Priorität auf einen sehr hohen Wert gesetzt wird, können Sie so eventuell Konfigurationsfragen vermeiden, aber Dienste, die auf Standardantworten angewiesen sind, welche jedoch auf Ihrem System nicht zutreffend sind, werden nicht erfolgreich starten.

<sup>2</sup>Zum Beispiel: DNS- oder DHCP-Dienste, besonders wenn keine Redundanz- oder Ersatzsysteme für den Fall eines Ausfalls vorhanden sind. Im Fall von DHCP-Diensten werden die Endbenutzer unter Umständen vom Netzwerk getrennt, wenn die Lease-Zeit niedriger ist als die, die für den Abschluß des Upgrade-Prozesses benötigt wird.

<sup>3</sup>Diese Funktionalität kann deaktiviert werden, indem der Parameter `panic=0` zu den Boot-Parametern hinzugefügt wird.

Folgende wesentliche Dinge sollten Sie prüfen: Vorhandensein der richtigen Gerätedateien in `/dev`, welche Module geladen sind (`cat /proc/modules`) und Fehler beim Laden von Treibern in der Ausgabe von `dmesg`. Die Ausgabe von `dmesg` wird Ihnen auch zeigen, welche Gerätedateien welchen Festplatten zugeordnet wurden; Sie sollten das mit der Ausgabe von `echo $ROOT` vergleichen, um sicherzustellen, dass die Wurzel des Dateisystems (`/`) auf dem erwarteten Gerät liegt.

Falls Sie das Problem beheben können, geben Sie `exit` ein, um die Debug-Shell zu beenden und mit dem Boot-Vorgang an der Fehlerstelle fortzufahren. Natürlich müssen Sie auch das zu Grunde liegende Problem beheben und die `Initrd` neu erzeugen, damit der Systemstart nicht beim nächsten Mal wieder fehlschlägt.

#### 4.1.4.2 Shell zur Fehleranalyse während des Bootens mit `systemd`

Falls das Booten unter `systemd` fehlschlägt, ist es über eine Änderung der Kernel-Befehlszeile möglich, eine Root-Shell zur Fehlersuche aufzurufen. Wenn das Booten grundsätzlich funktioniert, aber einige Dienste nicht starten, könnte es nützlich sein, `systemd.unit=rescue.target` zu den Kernel-Parametern hinzuzufügen.

In anderen Fällen bringt Ihnen der Kernel-Parameter `systemd.unit=emergency.target` zum frühest möglichen Zeitpunkt eine Root-Shell. Allerdings muss dazu das root-Dateisystem mit Lese-/Schreibrechten eingebunden werden. Sie müssen dies händisch erledigen mittels:

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

Sie finden weitere Informationen zur Fehlersuche bei fehlschlagenden Boot-Vorgängen unter `systemd` in dem [Diagnosing Boot Problems](https://freedesktop.org/wiki/Software/systemd/Debugging/) (<https://freedesktop.org/wiki/Software/systemd/Debugging/>)-Artikel.

#### 4.1.5 Vorbereiten einer sicheren Umgebung für das Upgrade

##### WICHTIG



Wenn Sie VPN-Dienste (wie zum Beispiel `tinc`) verwenden, sollten Sie davon ausgehen, dass diese während des Upgrades eine Zeit lang nicht verfügbar sein könnten. Bitte lesen Sie Abschnitt [4.1.3](#).

Für zusätzliche Sicherheit sollten Sie beim Upgrade aus der Ferne den Upgrade-Prozess in einer virtuellen Konsole des Programms `screen` durchführen, da bei temporären Verbindungsabbrüchen die Verbindung dann sicher wiederhergestellt werden kann und der Upgrade-Prozess somit nicht fehlschlägt.

#### 4.1.6 Kontrolle der Netzwerkschnittstellen-Bezeichnungen

Bei Systemen, die von früheren Veröffentlichungen hochgerüstet werden und die noch Netzwerkschnittstellen über Bezeichnungen wie `eth0` oder `wlan0` definieren, besteht das Risiko, dass sie nach der Umstellung auf Debian Buster die Netzwerkverbindung verlieren; lesen Sie dazu Abschnitt [5.1.6](#) bezüglich näherer Informationen für eine Migration auf die neuen Bezeichnungen.

## 4.2 Status der APT-Konfiguration überprüfen

Der Upgrade-Prozess, wie er in diesem Kapitel beschrieben wird, ist für „reine“ Debian Stable-Systeme konzipiert. Falls Ihre APT-Konfiguration noch weitere Paketquellen zusätzlich zu `stretch` enthält oder falls Sie Pakete aus anderen Debian-Veröffentlichungen oder von Drittanbietern installiert haben, sollten Sie diese Risikofaktoren eventuell durch Entfernen der Pakete ausräumen, um einen zuverlässigen Upgrade-Prozess sicherzustellen.

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.

Hier sind zwei Methoden aufgeführt, wie Sie Pakete finden können, die nicht original von Debian kommen, entweder mit **aptitude** oder **apt-forktracer**. Bitte beachten Sie, dass beide Methoden nicht immer zu 100% korrekte Resultate liefern (z.B. werden bei dem **aptitude**-Beispiel auch Pakete aufgelistet, die früher einmal von Debian angeboten wurden, jetzt aber nicht mehr (wie alte Kernel-Pakete)).

```
$ 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) (<https://www.debian.org/releases/stretch/releasenotes>) to upgrade to Debian 9 first.

Diese Anleitung geht davon aus, dass Ihr System auf die neueste Zwischenveröffentlichung von Stretch aktualisiert wurde. Falls dies nicht der Fall sein sollte oder Sie sich unsicher sind, folgen Sie den Anweisungen in Abschnitt [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 Abschnitt [A.2](#).

Es ist eine gute Idee, **veraltete Pakete** vor dem Upgrade zu entfernen.

### 4.2.1 Der Bereich für vorgeschlagene Aktualisierungen („proposed-updates“)

Wenn Sie `proposed-updates` in Ihren APT source-list-Dateien aufgeführt haben, sollten Sie das entfernen, bevor Sie versuchen, ein Upgrade Ihres Systems durchzuführen. Dies ist eine Vorsichtsmaßnahme, um die Zahl möglicher Konflikte zu reduzieren.

### 4.2.2 Inoffizielle Quellen

Falls auf Ihrem System Debian-fremde Pakete installiert sind, sollten Sie wissen, dass diese während des Upgrades aufgrund von Konflikten in den Abhängigkeiten entfernt werden könnten. Falls diese Pakete installiert wurden, indem eine zusätzliche Paketquelle in Ihre APT source-list-Dateien eingefügt wurde, sollten Sie überprüfen, ob das Archiv auch für Buster übersetzte Pakete anbietet und die Paketquelle gleichzeitig mit der Quelle für die Original-Debian-Pakete ändern.

Einige Benutzer haben möglicherweise *inoffizielle* rückportierte „neuere“ Versionen von Paketen, die *in Debian enthalten sind*, auf ihrem Stretch-System installiert. Diese Pakete werden wahrscheinlich während des Upgrades zu Problemen führen, da Dateikonflikte auftreten können<sup>4</sup>. Abschnitt [4.5](#) enthält Informationen, wie Sie mit Dateikonflikten umgehen, falls diese auftreten.

### 4.2.3 APT Pinning deaktivieren

Falls Sie APT so konfiguriert haben, dass bestimmte Pakete aus einer anderen Debian-Suite als Stable (z.B. aus Testing) installiert werden, müssen Sie unter Umständen Ihre APT-Pinning-Konfiguration (in `/etc/apt/preferences` und `/etc/apt/preferences.d/` gespeichert) ändern, um das Upgrade der Pakete aus der neuen Stable-Veröffentlichung zu erlauben. Weitere Informationen zu APT Pinning finden Sie in `apt_preferences(5)`.

### 4.2.4 Paketstatus überprüfen

Unabhängig von der Upgrade-Methode wird empfohlen, dass Sie zuerst überprüfen, ob alle Pakete in einem Status sind, der zum Upgrade geeignet ist. Der folgende Befehl wird Ihnen alle Pakete anzeigen, die im Status `halb-installiert` oder `Konfiguration-fehlgeschlagen` sind, und solche mit Fehler-Status:

```
# dpkg --audit
```

<sup>4</sup>Das Paketverwaltungssystem von Debian erlaubt es normalerweise nicht, dass ein Paket Dateien anderer Pakete entfernt oder ersetzt, es sei denn, es wurde definiert, dass es das andere Paket ersetzt.

Sie können auch den Status aller Pakete Ihres Systems mittels **aptitude** oder Befehlen der folgenden Form überprüfen:

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

oder

```
# dpkg --get-selections "*" > ~/derzeit-installierte-pakete.txt
```

Es ist erstrebenswert, alle hold-Markierungen („halten“; Markierung, dass ein Paket in dem Zustand belassen werden soll, in dem es ist; es würde nicht aktualisiert) vor dem Upgrade zu entfernen. Wenn irgendein Paket, das für das Upgrade unverzichtbar ist, auf hold steht, schlägt das Upgrade fehl.

Beachten Sie, dass **aptitude** verglichen mit **apt** oder **dselect** eine andere Methode verwendet, um Pakete als auf hold gesetzt zu registrieren. Sie können Pakete, für die die hold-Markierung gesetzt ist, mit **aptitude** identifizieren, indem Sie diesen Befehl verwenden:

```
# aptitude search "~ahold"
```

Um Pakete, die für **apt** auf hold gesetzt worden waren, zu identifizieren, sollten Sie dies verwenden:

```
# dpkg --get-selections | grep 'hold$'
```

Falls Sie ein Paket lokal verändert und neu kompiliert haben, und ihm dabei weder einen anderen Namen gegeben noch eine Epoche in die Versionsnummer eingefügt haben, müssen Sie es auf hold setzen, um zu verhindern, dass ein Upgrade für dieses Paket durchgeführt und es damit überschrieben wird.

Der „hold“-Paketstatus für **apt** kann mit folgenden Befehlen geändert werden: hold-Status setzen:

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

hold-Status löschen: ersetzen Sie `hold` durch `install`.

Falls etwas korrigiert werden muss, sorgen Sie am besten dafür, dass die APT source-list-Datei noch auf stretch verweist, wie in Abschnitt [A.2](#) erklärt.

## 4.3 Die APT source-list-Dateien vorbereiten

Bevor Sie das Upgrade beginnen, müssen Sie die APT source-list-Dateien (`/etc/apt/sources.list` und Dateien in `/etc/apt/sources.list.d/`) passend konfigurieren.

`apt` wird alle Pakete berücksichtigen, die über die konfigurierten Paketquellen gefunden werden, und das Paket mit der höchsten Versionsnummer installieren, wobei die Priorität auf dem ersten Eintrag in den Dateien liegt. Daher würden Sie bei der Existenz mehrerer Quellen typischerweise zuerst lokale Festplatten, dann CD-ROMs und schließlich ferne Archivspiegel angeben.

Eine Veröffentlichung kann sowohl mit ihrem Codenamen (z.B. `stretch`, `buster`) als auch mit ihrem Statusnamen (d.h. `oldstable`, `stable`, `testing`, `unstable`) benannt werden. Die Verwendung des Codenamens hat den Vorteil, dass Sie nie von neueren Veröffentlichungen überrascht werden, und wird daher hier verwandt. Natürlich bedeutet dies, dass Sie selbst auf Veröffentlichungsankündigungen achten müssen. Falls Sie stattdessen den Statusnamen verwenden, werden Sie nur eine große Menge an Aktualisierungen für Pakete sehen, wenn eine Veröffentlichung stattgefunden hat.

Debian betreibt zwei Ankündigungs-Mailinglisten, die Ihnen helfen, bezüglich der Informationen zu Debian-Veröffentlichungen auf dem aktuellen Stand zu bleiben:

- Wenn Sie die [Debian Announcement-Mailingliste](https://lists.debian.org/debian-announce/) (`https://lists.debian.org/debian-announce/`) abonnieren, bekommen Sie eine Informations-Mail, wenn Debian eine neue Veröffentlichung freigibt (wenn also z.B. Buster von stable in oldstable überführt wird).
- Über die [Debian Security-Announcement-Mailingliste](https://lists.debian.org/debian-security-announce/) (`https://lists.debian.org/debian-security-announce/`) erhalten Sie E-Mails, immer wenn Debian Sicherheitsankündigungen veröffentlicht.

### 4.3.1 APT-Internet-Quellen hinzufügen

Bei Neuinstallationen ist es Standardeinstellung, Debians APT-CDN-Service für APT zu benutzen; dies sollte sicherstellen, dass Pakete automatisch von dem (netzwerk-technisch gesehen) geografisch nächstliegenden Server heruntergeladen werden. Da dies noch ein relativ neuer Dienst ist, können vorhandene Installationen noch Konfigurationen haben, die direkt auf Debians Haupt-Internet-Server oder auf einen der Spiegel-Server verweisen. Falls noch nicht geschehen, wird empfohlen, dass Sie Ihre APT-Konfiguration auf den CDN-Service hin ändern.

Um den CDN-Service zu nutzen, fügen Sie eine Zeile wie die folgende zu Ihrer APT-Konfiguration hinzu (wir gehen hier davon aus, dass Sie `main` und `contrib` verwenden):

```
deb http://deb.debian.org/debian buster main contrib
```

Nachdem Sie die neuen Quellen hinzugefügt haben, deaktivieren Sie die bisher existierenden „deb“-Zeilen, indem Sie eine Raute (#) am Zeilenanfang einfügen.

Falls Sie über die direkte Angabe eines speziellen Spiegel-Servers, der netzwerk-technisch nahe bei Ihnen liegt, bessere Resultate erzielen, ist dies Art der Konfiguration aber nach wie vor ebenfalls möglich.

Adressen solcher Spiegel finden Sie auf <https://www.debian.org/distrib/ftplist> (suchen Sie nach dem Abschnitt „Liste von Debian-Spiegeln“).

Im Beispiel nehmen wir an, dass der für Sie am nächsten liegende Spiegel `http://mirrors.kernel.org` sei. Wenn Sie sich den Spiegel mit einem Webbrowser anschauen, werden Sie bemerken, dass die Hauptverzeichnisse wie folgt organisiert sind:

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

Um APT auf einen bestimmten Spiegel-Server zu konfigurieren, fügen Sie eine Zeile wie diese ein (diese verwendet wie oben `main` und `contrib`):

```
deb http://mirrors.kernel.org/debian buster main contrib
```

Beachten Sie, dass das „dists“ stillschweigend hinzugefügt wird und dass Argumente nach dem Namen der Veröffentlichung verwendet werden, um den Pfad aufzufächern, so dass er in mehrere unterschiedliche Verzeichnisse verweist.

Nach Hinzufügen der neuen Quellen deaktivieren Sie auch hier die bisher vorhandenen Einträge, indem Sie eine Raute (#) am Zeilenanfang einfügen.

### 4.3.2 APT-Quellen für einen lokalen Spiegel hinzufügen

Statt einen fernen Paketspiegel zu verwenden, können Sie auch Ihre APT source-list-Dateien anpassen, um einen Spiegel auf einer lokalen Platte zu nutzen (die z.B. über NFS eingebunden ist).

Beispielsweise könnte Ihr Paketspiegel unter `/var/local/debian/` liegen und über die folgenden Hauptverzeichnisse verfügen:

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

Um diesen Spiegel mit `apt` zu verwenden, fügen Sie die folgende Zeile zu Ihrer Datei `sources.list` hinzu:

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

Beachten Sie, dass das „dists“ stillschweigend hinzugefügt wird und dass Argumente nach dem Namen der Veröffentlichung verwendet werden, um den Pfad aufzufächern, so dass er in mehrere unterschiedliche Verzeichnisse verweist.

Nachdem Sie die neuen Quellen hinzugefügt haben, deaktivieren Sie die bisher existierenden Paketquellen in den APT source-list-Dateien, indem Sie eine Raute (#) am Zeilenanfang einfügen.



### 4.3.3 APT-Quellen für optische Medien hinzufügen

Falls Sie *ausschließlich* DVDs (oder CDs oder Blu-ray-Disks) verwenden möchten, kommentieren Sie die existierenden Einträge in allen APT source-list-Dateien aus, indem Sie am Zeilenanfang eine Raute (#) einfügen.

Stellen Sie sicher, dass es eine Zeile in `/etc/fstab` gibt, die das Einbinden Ihres CD-ROM-Laufwerks unter `/media/cdrom` bewirkt. Falls Ihr CD-ROM-Laufwerk beispielsweise `/dev/sr0` ist, sollte `/etc/fstab` eine Zeile wie diese enthalten:

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

Beachten Sie, dass es *keine Leerzeichen* zwischen den Begriffen `noauto,ro` im vierten Feld geben darf.

Um zu überprüfen, ob dies funktioniert, legen Sie eine CD/DVD ein und versuchen Sie, Folgendes auszuführen:

```
# mount /media/cdrom # dies wird die CD/DVD am Einbindungspunkt einbinden
# ls -alF /media/cdrom # dies sollte Ihnen das Wurzelverzeichnis der CD/DVD ↔
  anzeigen
# umount /media/cdrom # dies wird die Einbindung der CD/DVD wieder aufheben
```

Führen Sie als nächstes für jede Binär-CD/-DVD, die Sie von Debian haben, den Befehl

```
# apt-cdrom add
```

aus, um die Daten der CD/DVD zu der APT-Datenbank hinzuzufügen.

## 4.4 Upgrades von Paketen durchführen

Die empfohlene Methode zum Upgrade von vorherigen Debian-Versionen ist die Verwendung des Paketmanagement-Programms **apt**.

#### ANMERKUNG



**apt** ist für interaktive Nutzung gedacht und sollte nicht in Skripten verwendet werden. Dort sollten Sie stattdessen **apt-get** nutzen, weil dessen Ausgabe besser für die Abfrage in Skripten geeignet ist.

Vergessen Sie nicht, alle benötigten Partitionen (insbesondere `/` und `/usr`) zum Schreiben einzubinden. Verwenden Sie hierzu einen Befehl der Art:

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

Als nächstes sollten Sie noch einmal sicherstellen, dass die Quelleinträge für APT (in `/etc/apt/sources.list` und in allen Dateien in `/etc/apt/sources.list.d/`) entweder auf „buster“ oder auf „stable“ verweisen. Es sollte keine Quelleinträge für „stretch“ geben.

#### ANMERKUNG



Quellzeilen für eine CD-ROM könnten sich eventuell auf „unstable“ beziehen; dies mag zwar verwirrend erscheinen, Sie sollten dies jedoch *nicht* ändern.

### 4.4.1 Aufzeichnung der Sitzung

Es wird nachdrücklich empfohlen, dass Sie das Programm `/usr/bin/script` verwenden, um einen Mitschnitt der Upgrade-Sitzung zu erstellen. Falls dann ein Problem auftritt, haben Sie ein exaktes Protokoll der Ereignisse und können - falls notwendig - genaue Informationen in einem Fehlerbericht angeben. Um die Aufzeichnung zu beginnen, geben Sie

```
# script -t 2>~/upgrade-busterschritt1.time -a ~/upgrade-busterschritt1.script
```

oder vergleichbares ein. Falls Sie das Script erneut starten müssen (z.B. aufgrund eines Systemneustarts), zählen Sie den Wert für `schritt` hoch, um darzustellen, welchen Schritt des Upgrades Sie gerade aufzeichnen. Legen Sie die Mitschnittdatei nicht in einem temporären Verzeichnis wie `/tmp` oder `/var/tmp` ab (Dateien in diesen Verzeichnissen könnten während des Upgrades oder eines Systemstarts gelöscht werden).

Der Mitschnitt erlaubt es Ihnen auch, die Informationen durchzuschauen, die bereits aus dem Bildschirm herausgelaufen sind. Wenn Sie sich auf der System-Konsole befinden, schalten Sie auf VT2 um (mit `Alt + F2`) und verwenden Sie nach dem Anmelden etwas wie `less -R ~root/upgrade-buster.script`, um die Datei durchzuschauen.

Nach Beendigung des Upgrades können Sie `script` beenden, indem Sie `exit` an der Eingabeaufforderung eingeben.

`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`.

Falls Sie den Schalter `-t` für `script` verwendet haben, können Sie das Programm `scriptreplay` zum Abspielen der gesamten Sitzung verwenden:

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

### 4.4.2 Aktualisieren der Paketliste

Zuerst muss die Liste der verfügbaren Pakete für die neue Veröffentlichung abgerufen werden. Dies erledigen Sie mit dem folgenden Befehl:

```
# apt update
```

#### ANMERKUNG



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 Sicherstellen, dass genügend Speicherplatz für das Upgrade zur Verfügung steht

Sie müssen vor dem Upgrade sicherstellen, dass Sie genügend Platz auf Ihrer Festplatte verfügbar haben, wenn Sie wie in Abschnitt 4.4.5 beschrieben ein Upgrade des kompletten Systems starten. Als erstes wird jedes Paket, das zur Installation benötigt wird und über das Netz heruntergeladen werden muss, in `/var/cache/apt/archives` gespeichert (bzw. während des Downloads im Unterverzeichnis `partial/`). Sie müssen also sicherstellen, dass Sie auf der Partition, die `/var/` beinhaltet, genügend Platz haben, um temporär alle Pakete, die installiert werden sollen, herunterladen zu können. Nach dem Download benötigen Sie möglicherweise mehr Platz in anderen Partitionen, sowohl um die zu aktualisierenden Pakete zu installieren (diese könnten größere Binärdateien oder zusätzliche Daten enthalten)



als auch um Pakete zu installieren, die neu hinzukommen. Falls Sie nicht genügend freien Speicherplatz bereithalten, bleibt vielleicht ein System mit einem unvollständigen Upgrade zurück, das unter Umständen nur schwer wiederbelebt werden kann.

**apt** kann Ihnen detaillierte Informationen über den Festplattenplatz anzeigen, der für die Installation benötigt wird. Bevor Sie das Upgrade ausführen, können Sie sich die ungefähren Werte durch folgenden Befehl anschauen:

```
# apt -o APT::Get::Trivial-Only=true full-upgrade
[ ... ]
XXX aktualisiert, XXX neu installiert, XXX zu entfernen und XXX nicht ↔
aktualisiert.
Es müssen xxx.x MB an Archiven heruntergeladen werden.
Nach dieser Operation werden xxx MB Plattenplatz zusätzlich benutzt.
```

#### ANMERKUNG



Das Ausführen dieses Befehls zu Beginn des Upgrade-Prozesses könnte einen Fehler ausgeben (die Gründe sind in den folgenden Abschnitten beschrieben). In diesem Fall müssen Sie mit der Ausführung des Befehls warten, bis Sie das minimale System-Upgrade (wie in Abschnitt 4.4.4 beschrieben) durchgeführt haben, um den Platzbedarf abschätzen zu können.

Falls Sie nicht genügend Platz für das Upgrade haben, wird **apt** Sie mit einer Meldung wie dieser warnen:

```
F: Sie haben nicht genug Platz in /var/cache/apt/archives/.
```

In dieser Situation müssen Sie vorher manuell Platz schaffen. Sie können:

- Pakete löschen, die früher schon einmal für eine Installation heruntergeladen worden sind (in `/var/cache/apt/archives`). Durch das Leeren des Paket-Caches mit **apt clean** werden alle bereits heruntergeladenen Paketdateien gelöscht.
- Vergessene Pakete entfernen. Wenn Sie **aptitude** oder **apt** verwendet haben, um Pakete in Stretch manuell zu installieren, werden die Paketwerkzeuge dies registriert haben und können auch andere Pakete als unnötig markieren, die nur aufgrund von Abhängigkeiten installiert wurden und jetzt nicht mehr benötigt werden, weil ein Paket entfernt wurde. Es werden keine Pakete zur Entfernung vorgemerkt werden, die Sie manuell installiert haben. Um automatisch installierte und jetzt nicht mehr verwendete Pakete zu entfernen, führen Sie dies aus:

```
# apt autoremove
```

Sie können auch **debophan**, **debfoaster** oder **craft** verwenden, um unnötige Pakete zu finden. Entfernen Sie nicht blind die Pakete, die von diesen Programmen ausgegeben werden, speziell wenn Sie Optionen mit aggressiven Nicht-Standard-Werten verwenden, die dafür bekannt sind, falsch-positive Meldungen zu erzeugen. Es wird dringend empfohlen, dass Sie die Pakete, die zum Entfernen vorgeschlagen werden, kontrollieren (bezüglich Inhalt, Größe und Beschreibung), bevor Sie sie entfernen.

- Entfernen Sie Pakete, die viel Speicherplatz belegen und die aktuell nicht benötigt werden (Sie können sie nach dem Upgrade wieder installieren). Wenn Sie `popularity-contest` installiert haben, können Sie **popcon-largest-unused** verwenden, um die Pakete aufzulisten, die derzeit nicht verwendet werden und den meisten Platz verbrauchen. Um die Pakete ausfindig zu machen, die schlicht den meisten Festplattenspeicher in Anspruch nehmen, verwenden Sie **dpigs** (aus dem `debian-goodies`-Paket) oder **wajig** (führen Sie `wajig size` aus). Desweiteren können Sie diese Pakete auch mit `aptitude` finden. Starten Sie dazu **aptitude** im Terminal-Modus, wählen Sie

Ansichten → Neue einfache Paketansicht, drücken Sie **I** und geben Sie `~i` ein, drücken Sie dann **S** und geben Sie `~installsize` ein. Nun wird Ihnen eine schöne Liste angezeigt, mit der Sie arbeiten können.

- Entfernen von Übersetzungen und Standortanpassungsdateien aus dem System, falls diese nicht benötigt werden. Sie können das Paket `localepurge` installieren und so konfigurieren, dass nur einige ausgewählte Gebietsschemata („locales“) im System verbleiben. Dies wird den unter `/usr/share/locale` benötigten Plattenplatz reduzieren.
- System-Protokolldateien (die unter `/var/log/` liegen) vorübergehend auf ein anderes System verschieben oder dauerhaft löschen.
- Ein temporäres `/var/cache/apt/archives` verwenden: Sie können vorübergehend ein Cache-Verzeichnis auf einem anderen Dateisystem benutzen (USB-Speicher, provisorisch angeschlossene Festplatte, ein bereits anderweitig benutztes Dateisystem ...).

#### ANMERKUNG



Benutzen Sie jedoch kein per NFS eingebundenes Netzlaufwerk, da die Netzwerkverbindung während des Upgrades unterbrochen werden könnte.

Falls Sie zum Beispiel eine USB-Festplatte haben, die in `/media/usbkey` eingebunden ist:

1. entfernen Sie die Pakete, die unter Umständen bereits früher für Installationen heruntergeladen worden sind:

```
# apt clean
```

2. kopieren Sie das Verzeichnis `/var/cache/apt/archives` auf die USB-Festplatte:

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

3. binden Sie das temporäre Cache-Verzeichnis in dem vorhandenen ein:

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

4. stellen Sie nach dem Upgrade das ursprüngliche `/var/cache/apt/archives`-Verzeichnis wieder her:

```
# umount /media/usbkey/archives
```

5. entfernen Sie das verbleibende `/media/usbkey/archives`.

Sie können das temporäre Cache-Verzeichnis auf jedem Dateisystem erstellen, das auf Ihrem System eingebunden ist.

- Führen Sie ein minimales Upgrade (siehe Abschnitt 4.4.4) oder andere Teil-Upgrades des Systems durch, gefolgt von einem vollständigen Upgrade. Dies schafft die Möglichkeit, das System stückweise zu aktualisieren und erlaubt es Ihnen, den Paket-Cache vor dem vollständigen Upgrade nochmals zu leeren.

Beachten Sie, dass es ratsam ist, die APT source-list-Dateien zurück auf stretch zu ändern (wie in Abschnitt A.2 beschrieben), um Pakete sicher entfernen zu können.

#### 4.4.4 Minimales System-Upgrade

In einigen Fällen wird durch das direkte Ausführen des vollständigen Upgrades (wie unten beschrieben) eine große Anzahl von Paketen entfernt, die Sie eigentlich behalten möchten. Wir empfehlen deshalb einen zweiseitigen Upgrade-Prozess: als erstes ein minimales Upgrade, um diese Konflikte zu umgehen und anschließend ein vollständiges Upgrade wie in Abschnitt 4.4.5 beschrieben.

Führen Sie dazu zuerst dies aus:

```
# apt-get upgrade
```

Dies hat den Effekt, dass für diejenigen Pakete ein Upgrade durchgeführt wird, für die dies möglich ist, ohne dass irgendwelche anderen Pakete entfernt oder installiert werden müssen.

Solch ein minimales System-Upgrade kann auch nützlich sein, wenn auf dem System freier Festplattenplatz knapp ist und aus diesem Grund ein komplettes Upgrade nicht durchgeführt werden kann.

Falls das `apt-listchanges`-Paket installiert ist, wird es (in seiner Standard-Konfiguration) alle wichtigen Informationen über aktualisierte Pakete in einem Pager anzeigen, nachdem die Pakete heruntergeladen wurden. Drücken Sie `q`, nachdem Sie alles gelesen haben, um den Pager zu beenden und das Upgrade fortzusetzen.

#### 4.4.5 Upgrade des Systems

Wenn Sie die vorherigen Schritte hinter sich gebracht haben, Sie sind bereit für den eigentlichen Hauptteil des Upgrades. Führen Sie aus:

```
# apt full-upgrade
```

Dadurch wird ein vollständiges Upgrade des Systems durchgeführt, also die Installation der neuesten verfügbaren Versionen aller Pakete und die Auflösung aller möglichen Änderungen bei den Abhängigkeiten zwischen Paketen der verschiedenen Veröffentlichungen. Falls nötig werden einige neue Pakete installiert (üblicherweise neue Bibliotheksversionen oder umbenannte Pakete) sowie veraltete Pakete entfernt, die Konflikte verursachen.

Falls Sie ein Upgrade von einem Satz CDs/DVDs/BDs durchführen, werden Sie an verschiedenen Stellen des Upgrade-Prozesses aufgefordert, bestimmte Disks einzulegen. Sie müssen eventuell ein und dieselbe Disk mehrmals einlegen; dies liegt daran, dass einige Pakete mit gegenseitiger Wechselbeziehung zueinander über verschiedene Disks verteilt sind.

Neue Versionen von bereits installierten Paketen, die nicht aktualisiert werden können, ohne den Installationsstatus eines anderen Pakets zu ändern, werden in ihrer derzeitigen Version belassen (sie werden als „zurückgehalten“ angezeigt). Dies kann aufgelöst werden, indem Sie entweder `aptitude` verwenden, um diese Pakete zur Installation vorzumerken, oder indem Sie `apt install paketname` versuchen.

### 4.5 Mögliche Probleme während des Upgrades

Die folgenden Abschnitte beschreiben bekannte Probleme, die während des Upgrades auf Buster auftreten können.

#### 4.5.1 `dist-upgrade` schlägt fehl mit „Could not perform immediate configuration“

In einigen Fällen kann der Schritt `apt full-upgrade` nach dem Heruntergeladen der Pakete fehlschlagen mit der Meldung:

```
E: Could not perform immediate configuration on 'paket'. Please see man 5 apt. ←  
conf under APT::Immediate-Configure for details.
```

Falls dies passiert, sollte es möglich sein, mit `apt full-upgrade -o APT::Immediate-Configure=0` das Upgrade fortzusetzen.

Eine andere Möglichkeit, dies zu umgehen ist, vorübergehend sowohl stretch- wie auch buster-Quellen in Ihren APT source-list-Dateien anzugeben und danach **apt update** auszuführen.

### 4.5.2 Zu erwartende Paketentfernungen

Der Upgrade-Prozess auf Buster könnte auch das Entfernen von Paketen im System bedeuten. Die exakte Liste der zu entfernenden Pakete variiert in Abhängigkeit von den Paketen, die Sie installiert haben. Diese Veröffentlichungshinweise geben grundsätzliche Hinweise über diese Paketentfernungen, falls Sie aber Zweifel haben, wird empfohlen, dass Sie die Liste zu entfernender Pakete, die von den einzelnen Upgrade-Methoden vorgeschlagen werden, kontrollieren, bevor Sie fortfahren. Weitere Informationen über veraltete Pakete in Buster finden Sie in Abschnitt 4.8.

### 4.5.3 Conflicts- oder Pre-Depends-Schleifen

Manchmal ist es nötig, die Option `APT::Force-LoopBreak` in APT zu aktivieren, um die Möglichkeit zu haben, ein zwingend nötiges Paket vorübergehend entfernen zu können, falls das Problem einer Conflicts-/Pre-Depends-Schleife besteht. **apt** wird Sie über solch eine Problematik informieren und das Upgrade abbrechen. Sie setzen diese Option, indem Sie `-o APT::Force-LoopBreak=1` in den **apt**-Befehl einfügen.

Es ist möglich, dass die Abhängigkeitsstruktur eines Systems so beschädigt ist, dass ein manuelles Eingreifen nötig ist. Dies erfordert üblicherweise die Verwendung von **apt** oder

```
# dpkg --remove paketname
```

um einige der beschädigten Pakete zu eliminieren, oder

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

In extremen Fällen müssen Sie eventuell die Neuinstallation eines Pakets erzwingen; verwenden Sie dazu einen Befehl wie

```
# dpkg --install /pfad/zu/paketname.deb
```

### 4.5.4 Dateikonflikte

Dateikonflikte sollten nicht auftauchen, wenn Sie ein Upgrade auf einem „reinen“ Stretch-System durchführen, können aber vorkommen, wenn Sie inoffizielle Backports installiert haben. Ein Dateikonflikt resultiert in einem Fehler wie:

```
Entpacken von <irgendein-paket1> (aus <irgendein-paket1-dateiname>) ...
dpkg: Fehler beim Bearbeiten von <irgendein-paket1> (--install):
  Versuch, <name-irgendeiner-datei> zu überschreiben,
  welches auch in Paket <irgendein-paket2> ist
dpkg-deb: Unterprozess paste mit Signal (Broken pipe) getötet
Fehler traten auf beim Bearbeiten von:
<irgendein-paket1>
```

Sie können versuchen, einen Dateikonflikt zu lösen, indem Sie zwangsweise das Paket entfernen, das in der *letzten* Zeile der Fehlermeldung genannt wird:

```
# dpkg -r --force-depends paketname
```

Nachdem Sie die Probleme behoben haben, sollte es möglich sein, das Upgrade fortzusetzen, indem Sie die oben beschriebenen **apt**-Befehle nochmals ausführen.

### 4.5.5 Konfigurationsänderungen

Während des Upgrades werden Ihnen Fragen gestellt, die die Konfiguration oder Neukonfiguration verschiedener Pakete betreffen. Wenn Sie gefragt werden, ob Dateien in den Verzeichnissen `/etc/init.d` oder die Datei `/etc/manpath.config` durch die Version des Paketbetreuers ersetzt werden sollen, ist es für gewöhnlich nötig, mit „yes“ (ja) zu antworten, um die Konsistenz des Systems sicherzustellen. Sie können jederzeit zu den alten Versionen der Konfigurationsdateien zurückkehren, da diese mit der Erweiterung `.dpkg-old` gesichert werden.

Falls Sie sich nicht sicher sind, was Sie tun sollen, schreiben Sie den Namen des Pakets oder der Datei auf und kümmern Sie sich später darum. Sie können die Mitschnittdatei durchsuchen, um die Informationen erneut zu betrachten, die zum Zeitpunkt des Upgrades auf dem Bildschirm angezeigt wurden.

### 4.5.6 Ändern der aktuellen Sitzung auf die Konsole

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.

Um die Konsole wiederherzustellen, auf der der Upgrade-Prozess läuft, müssen Sie `Strg+Alt+F1` betätigen (wenn Sie vom grafischen Startbildschirm zur 1. virtuellen Konsole wechseln möchten) oder `Alt+F1` (wenn Sie sich auf einer virtuellen Text-Konsole befinden). Ersetzen Sie dabei `F1` durch die Funktionstaste, die der Konsole zugeordnet ist, auf der der Upgrade-Prozess läuft. Sie können auch `Alt+Pfeiltaste-Links` oder `Alt+Pfeiltaste-Rechts` verwenden, um zwischen den verschiedenen Textmodus-Konsolen hin- und herzuschalten.

## 4.6 Upgrade des Kernels und zugehöriger Pakete

Dieser Abschnitt beschreibt, wie Sie ein Upgrade des Kernels durchführen und weist auf potenzielle Probleme hin, die diesen Vorgang betreffen. Sie können entweder eines der von Debian angebotenen `linux-image-*`-Pakete installieren oder einen eigenen Kernel aus den Quellen selbst kompilieren.

Beachten Sie, dass viele der Informationen in diesem Abschnitt auf der Annahme basieren, dass Sie einen der modularen Debian-Kernel zusammen mit `initramfs-tools` und `udev` verwenden. Falls Sie sich entscheiden, einen eigenen selbst erstellten Kernel zu benutzen, der keine `Initrd` benötigt, oder wenn Sie einen anderen `Initrd`-Generator verwenden, könnten einige der Informationen für Sie nicht relevant sein.

### 4.6.1 Ein Kernel-Metapaket installieren

Wenn Sie ein Distributions-Upgrade mit (**apt full-upgrade**) von Stretch auf Buster durchführen, wird dringend empfohlen, ein `linux-image-*`-Metapaket zu installieren, falls noch nicht geschehen. Diese Metapakete werden während des Upgrade-Prozesses automatisch eine neue Kernel-Version installieren. Ob Sie eins installiert haben, können Sie verifizieren mit:

```
# dpkg -l "linux-image*" | grep ^ii | grep -i meta
```

Falls nichts angezeigt wird, müssen Sie entweder ein neues `linux-image`-Paket von Hand installieren oder Sie installieren ein `linux-image`-Metapaket. Eine Liste verfügbarer `linux-image`-Metapakete bekommen Sie mit:

```
# 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
```

Sie sollten dann `apt install` verwenden, um es zu installieren. Sobald dieser neue Kernel installiert ist, sollten Sie sobald wie möglich einen Neustart durchführen, um von der neuen Kernel-Version zu profitieren. Lesen Sie aber Abschnitt 5.1.12, bevor Sie nach dem Upgrade den ersten Reboot durchführen.

Für alle Experimentierfreudigen gibt es einen einfachen Weg, einen eigenen angepassten Kernel unter Debian zu kompilieren. Installieren Sie die Kernel-Quellen aus dem `linux-source`-Paket. Sie können dann das Target `dep-pkg` zur Erstellung eines Binär-Pakets verwenden. Weitere Informationen finden Sie im [Debian Linux Kernel-Handbuch](https://kernel-team.pages.debian.net/kernel-handbook/) (<https://kernel-team.pages.debian.net/kernel-handbook/>), das es auch als `debian-kernel-handbook`-Paket gibt.

Falls möglich, wäre es ein Vorteil, wenn Sie das Kernel-Paket separat vom Rest des Systems aktualisieren, um die Wahrscheinlichkeit eines nicht-bootfähigen Systems zu reduzieren. Beachten Sie, dass dies nur nach dem minimalen System-Upgrade (siehe Abschnitt 4.4.4) durchgeführt werden sollte.

## 4.7 Vorbereiten auf die nächste Veröffentlichung

Nach dem Upgrade gibt es einige Dinge, die Sie tun können, um für die nächste Veröffentlichung vorbereitet zu sein.

- Entfernen Sie nicht mehr benötigte und veraltete Pakete wie in Abschnitt 4.4.3 und Abschnitt 4.8 beschrieben. Sie sollten kontrollieren, welche Konfigurationsdateien diese Pakete benutzen und in Betracht ziehen, die Pakete vollständig zu entfernen, um die Konfigurationsdateien loszuwerden. Lesen Sie auch Abschnitt 4.7.1.

### 4.7.1 Vollständiges Löschen entfernter Pakete

Es ist grundsätzlich empfehlenswert, entfernte Pakete vollständig (inkl. der Konfigurationsdateien) zu löschen. Dies ist besonders relevant, wenn sie im Rahmen eines früheren Upgrades entfernt wurden (z.B. bei dem Upgrade auf Stretch) oder bei Paketen von Drittanbietern. Speziell alte `init.d`-Skripte sind dafür bekannt, Probleme zu verursachen.

#### ACHTUNG



Das vollständige Löschen eines Pakets wird grundsätzlich auch dessen Logdateien vom System entfernen, daher sollten Sie sie eventuell vorher sichern.

Folgender Befehl zeigt eine Liste aller entfernten Pakete an, deren Konfigurationsdateien noch auf dem System vorhanden sind (falls zutreffend):

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

Die Pakete können mittels **apt purge** vollständig gelöscht werden. Wenn wir davon ausgehen, dass Sie alle in einem Rutsch löschen möchten, können Sie folgenden Befehl verwenden:

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

Wenn Sie `aptitude` verwenden, können Sie alternativ zu obigen Befehlen auch folgendes nutzen:

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

## 4.8 Veraltete Pakete

Mit Buster werden viele neue Pakete eingeführt, jedoch werden auch einige alte Pakete, die in Stretch noch existierten, ausgelassen oder weggelassen. Es wird keine Möglichkeit eines Upgrades für diese veralteten Pakete geben. Selbst wenn nichts Sie davon abhalten kann, ein veraltetes Paket weiter zu benutzen, falls Sie dies wünschen, wird das Debian-Projekt bei diesen Paketen üblicherweise die Unterstützung für Sicherheitsaktualisierungen ein Jahr nach der Veröffentlichung von Buster einstellen<sup>5</sup> und auch sonst in der Zwischenzeit keine Unterstützung dafür anbieten. Es wird empfohlen, die Pakete gegen die empfohlenen Alternativen (falls verfügbar) auszutauschen.

Es gibt viele Gründe, warum Pakete aus der Distribution entfernt worden sein könnten: sie wurden von den Originalautoren nicht mehr betreut; es ist kein Debian-Entwickler mehr daran interessiert, sie zu betreuen; die Funktionalität, die sie bieten, ist durch andere Software (oder eine neuere Version) ersetzt worden, oder sie wurden (aufgrund von Fehlern darin) als nicht mehr passend für Buster angesehen. Im letzten Fall könnten sie trotzdem noch in der „unstable“-Distribution vorhanden sein.

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

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

Die **Debian-Fehlerdatenbank** (<https://bugs.debian.org/>) bietet oft zusätzliche Informationen, warum ein Paket entfernt wurde. Sie sollten sowohl die archivierten Fehlerberichte für das Paket selbst als auch für das **Pseudo-Paket ftp.debian.org** (<https://bugs.debian.org/cgi-bin/pkgreport.cgi?pkg=ftp.debian.org&archive=yes>) kontrollieren.

Eine Liste veralteter Pakete für Buster finden Sie unter Abschnitt **5.1.10**.

### 4.8.1 Übergangs-Dummy-Pakete

Einige Pakete aus Stretch könnten in Buster durch Übergangs-Dummy-Pakete ersetzt worden sein; das sind leere Platzhalter-Pakete, die lediglich dazu gedacht sind, um ein Upgrade zu vereinfachen. Wenn zum Beispiel eine Anwendung, die vorher nur aus einem einzigen Paket bestand, in mehrere Pakete aufgeteilt wurde, kann ein Übergangspaket bereitgestellt werden, das den gleichen Namen wie das alte Paket hat sowie entsprechende Abhängigkeiten, die dazu führen, dass alle neuen Pakete installiert werden. Nachdem dieser Installationsvorgang stattgefunden hat, kann das Übergangspaket problemlos entfernt werden.

Die Paketbeschreibungen für Übergangs-Dummy-Pakete enthalten normalerweise einen Hinweis auf ihren Zweck. Jedoch sind diese Beschreibungen nicht standardisiert; insbesondere sind einige Dummy-Pakete nicht dazu gedacht, nach dem Upgrade entfernt zu werden, sondern dienen stattdessen dazu, eine größere Programm-Suite vollständig zu installieren oder die aktuell verfügbare Version eines Programms zu verfolgen. Vielleicht ist **deborphan** mit einer der `--guess-*`-Optionen für Sie nützlich (z.B. `--guess-dummy`), um solche Übergangs-Pakete auf Ihrem System zu finden.

---

<sup>5</sup>So lange es keine andere Veröffentlichung in diesem Zeitraum gibt. Typischerweise werden zu jeder Zeit nur zwei stabile Veröffentlichungen mit Sicherheitsaktualisierungen unterstützt.





# Kapitel 5

## Dinge, die Sie über Buster wissen sollten

Manchmal haben Änderungen, die in einer neuen Veröffentlichung eingebracht werden, Nebeneffekte, die wir ohne größeren Aufwand nicht vermeiden können, oder dies würde Fehler an anderen Stellen verursachen. Dieses Kapitel dokumentiert die uns bekannten Probleme. Bitte lesen Sie auch die Errata, die relevanten Paketdokumentationen, Fehlerberichte und weitere Informationen in Abschnitt [6.1](#).

### 5.1 Upgrade-spezifische Themen für Buster

Dieser Abschnitt behandelt Themen, die für ein Upgrade von Stretch auf Buster relevant sind.

#### 5.1.1 Mount-Option `hidepid` für `procs` nicht mehr unterstützt

Die mount-Option `hidepid` für `/proc` ist bekannt dafür, Probleme mit aktuellen Versionen von `systemd` zu verursachen, und wird von den `Systemd`-Autoren als nicht unterstützte Konfiguration angesehen. Benutzer, die ihre `/etc/fstab`-Datei modifiziert haben, um diese Option zu aktivieren, werden aufgefordert, diese vor dem Upgrade zu deaktivieren, um sicherzustellen, dass Login-Sitzungen mit Buster funktionieren. (Ein möglicher Weg, um dies wieder zu aktivieren, wird auf der [Hardening](https://wiki.debian.org/Hardening#Mounting_.2Fproc_with_hidepid) ([https://wiki.debian.org/Hardening#Mounting\\_.2Fproc\\_with\\_hidepid](https://wiki.debian.org/Hardening#Mounting_.2Fproc_with_hidepid))-Seite im Wiki erklärt.)

#### 5.1.2 Start von `ybind` mit `-no-dbus` schlägt fehl

Die Standardoptionen von `ybind` wurden geändert. Wenn Sie selbst jedoch diese Datei verändert haben, werden die alten Optionen nicht aktualisiert und Sie müssen sicherstellen, dass die Option `YPBINDARGS=` in `/etc/default/nis` nicht mehr `-no-dbus` enthält. Falls `-no-dbus` enthalten ist, wird der Start von `ybind` fehlschlagen, und Sie können sich möglicherweise nicht mehr anmelden. Weitere Informationen finden Sie im [Fehlerbericht #906436](https://bugs.debian.org/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) (<https://bugs.debian.org/935492>).

#### 5.1.4 Authentifizierung von `sshd` schlägt fehl

Die Semantik von `PubkeyAcceptedKeyTypes` sowie die verwandten `HostbasedAcceptedKeyTypes`-Optionen für `sshd` wurden geändert. Sie legen jetzt Signatur-Algorithmen fest, die für die jeweiligen Authentifizierungsmechanismen akzeptiert werden. Früher hingegen wurden dort die akzeptierten Schlüsseltypen angegeben. Dieser Unterschied ist relevant, wenn die RSA/SHA2-Signatur-Algorithmen

`rsa-sha2-256`, `rsa-sha2-512` sowie deren Zertifikats-Gegenstücke verwendet werden. Konfigurationen, die diese Optionen überschreiben, aber dabei diese Algorithmus-Bezeichnungen nicht enthalten, können zu unerwarteten Fehlern bei der Authentifizierung führen.

Bei Konfigurationen, die den Standardwert für diese Optionen verwenden, besteht kein Handlungsbedarf.

### 5.1.5 Daemon-Prozesse starten nicht mehr oder das System scheint während des Boot-Vorgangs zu hängen

Da `systemd` für den Boot-Vorgang eine gewisse Menge an Entropy benötigt und der Kernel entsprechende Aufrufe blockiert, wenn nicht genügend Entropy zur Verfügung steht, kann das System während des Bootens hängen bleiben, bis das Randomness-Subsystem korrekt initialisiert ist (`random: crng init done`). Auf amd64-Systemen, die die `RDRAND`-Anweisung unterstützen, wird dieses Problem durch den Debian-Kernel umgangen, indem diese Anweisung standardmäßig verwendet wird (`CONFIG_RANDOM_TRUST_CPU`).

Auf Nicht-amd64-Systemen und einigen Arten virtueller Maschinen muss eine andere Entropy-Quelle bereitgestellt werden, um weiterhin schnell booten zu können. Hierfür wurde innerhalb des Debian-Projekts `haveged` ausgewählt; es kann eine gute Option sein, wenn Hardware-Entropy auf dem System nicht verfügbar ist. Auf virtuellen Maschinen können Sie in Erwägung ziehen, Entropy mittels `virtio_rng` vom Host an die virtuelle Maschine durchzureichen.

Falls Sie dies erst lesen, nachdem das Upgrade eines fernen Systems auf buster bereits durchgeführt wurde, pingt Sie das System über das Netzwerk fortwährend an, da hierdurch Entropy zum Randomness-Pool des Systems hinzugefügt wird und das System dann eventuell wieder per SSH erreichbar wird.

Weitere Details finden Sie im [Wiki](https://wiki.debian.org/BoottimeEntropyStarvation) (<https://wiki.debian.org/BoottimeEntropyStarvation>); für zusätzliche verfügbare Optionen besuchen Sie [DLange's overview of the issue](https://daniel-lange.com/archives/152-hello-buster.html) (<https://daniel-lange.com/archives/152-hello-buster.html>).

### 5.1.6 Migration von altbekannten Netzwerkschnittstellen-Namen

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) (<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).

Um die neuen Namen zu erfahren, die nach der Migration verwendet würden, suchen Sie zunächst die alten Namen der entsprechenden Schnittstellen heraus:

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

Prüfen Sie jeden dieser Namen, ob er in irgendwelchen Konfigurationsdateien verwendet wird, und welchen Namen das `udev`-System dafür vergeben würde:

```
$ 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.)

Sobald sie bereit sind für die Umstellung, deaktivieren Sie `70-persistent-net.rules`, entweder indem Sie diese Datei umbenennen oder entsprechende Zeilen darin auskommentieren. Bei virtuellen

Maschinen müssen Sie die Datei `/etc/systemd/network/99-default.link` und (falls Sie virtio-Netzwerkgeräte benutzen) `/etc/systemd/network/50-virtio-kernel-names.link` entfernen. Bauen Sie danach die `initrd` neu mit

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

und starten Sie das System neu. Es sollte nun Netzwerk-Schnittstellen-Namen nach dem neuen Namensschema nutzen. Passen Sie verbleibende Konfigurationsdateien an und testen Sie Ihr System.

See [the wiki](https://wiki.debian.org/NetworkInterfaceNames) (<https://wiki.debian.org/NetworkInterfaceNames>), [upstream documentation](https://www.freedesktop.org/software/systemd/man/systemd.net-naming-scheme.html) (<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-Standard-Version und erhöhtes Sicherheits-Level

Verschiedenen Sicherheitsempfehlungen folgend, wurde die standardmäßig als Minimum erforderliche TLS-Version von TLSv1 auf TLSv1.2 erhöht.

Das als Standard eingestellte Sicherheits-Level für TLS-Verbindungen wurde ebenfalls von Level 1 auf Level 2 erhöht. Dies bedeutet einen Umstieg vom 80-Bit Sicherheits-Level auf ein 112-Bit Sicherheits-Level und erfordert RSA- und DHE-Schlüssel mit mindestens 2048 Bit Länge, ECC-Schlüssel mit mindestens 224 Bit Länge sowie SHA-2.

Die systemweiten Einstellungen können in `/etc/ssl/openssl.cnf` geändert werden. Anwendungen können auch spezielle Möglichkeiten verwenden, um die Standardeinstellungen zu überschreiben.

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)) ([https://manpages.debian.org/buster/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)) ([https://manpages.debian.org/buster/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)) ([https://manpages.debian.org/buster/ciphers\(1ssl\)](https://manpages.debian.org/buster/ciphers(1ssl))) and [config\(5ssl\)](https://manpages.debian.org/buster/config(5ssl)) ([https://manpages.debian.org/buster/config\(5ssl\)](https://manpages.debian.org/buster/config(5ssl))).

Die systemweiten Standardeinstellungen in `/etc/ssl/openssl.cnf` können mittels folgender Einträge auf die vorherigen Werte zurückgestellt werden:

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

Es wird empfohlen, dass Sie die Verantwortlichen der anderen, fernen Seite der Verbindung kontaktieren, falls diese Standardwerte Probleme verursachen.

### 5.1.9 Einige Anwendungen funktionieren nicht in GNOME mit Wayland

GNOME in Debian Buster verwendet als Standard-Display-Server jetzt nicht mehr Xorg, sondern Wayland (siehe Abschnitt 2.2.11). Einige Anwendungen (wie der populäre Paketmanager `synaptic`, die Standard-Eingabemethode für vereinfachtes Chinesisch `fcitx`, sowie die meisten Programme zur Aufzeichnung von Bildschirminhalten) wurden noch nicht passend aktualisiert, so dass sie noch nicht korrekt mit Wayland funktionieren. Um solche Pakete nutzen zu können, müssen Sie sich mit einer GNOME on Xorg-Sitzung anmelden.

### 5.1.10 Nennenswerte veraltete Pakete

Hier eine Liste bekannter und erwähnenswerter veralteter Pakete (lesen Sie hierzu auch Abschnitt 4.8). Zu diesen Paketen gehören:

- Das Paket `mcelog` wird von Kernel-Versionen über 4.12 nicht mehr unterstützt. Stattdessen kann `rasdaemon` verwendet werden.
- `Revelation`, das verwendet wird, um Passwörter zu speichern, ist in Debian Buster nicht mehr enthalten. Wenn Sie Ihre Passwörter vorher mit `revelation` in XML-Dateien exportiert haben, kann `keepass2` diese importieren. Bitte stellen Sie sicher, dass Sie vor dem Upgrade Ihre Daten in solch eine Datei exportieren, um den Verlust Ihrer Passwörter zu vermeiden.
- Das Paket `phpmyadmin` ist in Buster nicht mehr enthalten.
- `ipsec-tools` und `raccoon` wurden aus Buster entfernt, da ihr Quellcode weit hinterher hing bei der Adaption neuer Bedrohungsmuster.

Benutzern wird empfohlen, zu `libreswan` zu migrieren, da es eine breitere Protokollkompatibilität bietet und von den Originalautoren aktiv weiterentwickelt wird.

`libreswan` sollte bezüglich der Kommunikationsprotokolle vollständig kompatibel sein, da es die Obermenge der von `raccoon` unterstützten Protokolle ebenfalls implementiert hat.

- Der einfache MTA `ssmtp` wurde aus Buster entfernt. Der Grund hierfür ist, dass er derzeit keine TLS-Zertifikate validiert; Näheres im Fehlerbericht #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 Missbilligte Komponenten für Buster

Mit der nächsten Veröffentlichung von Debian 11 (Codename Bullseye) werden einige Funktionalitäten missbilligt sein. Nutzer müssen auf andere Alternativen umsteigen, um Schwierigkeiten nach dem Upgrade auf Debian 11 zu vermeiden.

Dazu gehören folgende Funktionalitäten:

- `debianPython 2` wird von den Originalautoren ab dem 01. Januar 2020 (<https://www.python.org/dev/peps/pep-0373/>) nicht mehr unterstützt. Debian hofft, das `python-2.7`-Paket in Debian 11 entfernen zu können. Falls Nutzer Funktionalitäten haben, die auf `python` beruhen, sollten sie sich darauf vorbereiten, auf `python3` zu migrieren.
- `Icinga 1.x` hat am 31.12.2018 bei den Upstream-Autoren sein Lebensende erreicht. In Debian ist das `icinga`-Paket zwar noch enthalten, Nutzer sollten aber während des Lebenszyklus von Debian Buster nach `Icinga 2` (im `icinga2`-Paket) und `Icinga Web 2` (im `icingaweb2`-Paket) migrieren. Das `icinga2-classicui`-Paket kann genutzt werden, um das Icinga-CGI-Web-Interface der Version 1.x mit `Icinga 2` zu verwenden, aber dies wird mit der `Icinga`-Version 2.11 entfallen. Stattdessen sollte `Icinga Web 2` eingesetzt werden.
- Die Version 3 des Mailinglisten-Managers `Mailman` ist in dieser Veröffentlichung neu verfügbar. `Mailman` wurde in mehrere Komponenten aufgesplittet; der Kern ist im `mailman3`-Paket enthalten, während über das Metapaket `mailman3-full` die komplette Suite installiert werden kann.

Die alte Version Mailman 2.1 bleibt in dieser Debian-Veröffentlichung im Paket `mailman` enthalten, so dass Sie vorhandene Installationen nach eigenem Ermessen auf die neue Version migrieren können. Mailman 2.1 wird für absehbare Zeit funktionsfähig gehalten, allerdings keine größeren Änderungen oder Verbesserungen mehr bekommen. Sobald die Upstream-Autoren diesen Zweig nicht mehr unterstützen, wird er mit der nächsten darauf folgenden Debian-Veröffentlichung auch aus Debian verschwinden.

Alle werden aufgefordert, auf die moderne und in aktueller Entwicklung stehende Version Mailman 3 hochzurüsten.

- Die Pakete `spf-milter-python` und `dkim-milter-python` werden von den Originalautoren nicht mehr aktiv weiterentwickelt, aber die Nachfolgekompakte `pyspf-milter` und `dkimpy-milter` (die auch neue zusätzliche Funktionalitäten enthalten), sind in Debian Buster enthalten. Nutzer sollten auf die neuen Pakete migrieren, bevor die alten in Debian Bullseye entfernt werden.

### 5.1.12 Dinge, die vor dem Neustart erledigt werden sollten

Wenn `apt full-upgrade` beendet ist, sollte das „formale“ Upgrade abgeschlossen sein. Nach dem Upgrade auf Buster gibt es keine besonderen Aktionen, die vor dem nächsten Neustart erledigt werden müssen.

### 5.1.13 SysV-init betreffende Pakete nicht länger benötigt

#### ANMERKUNG



Dieser Abschnitt betrifft Sie nicht, wenn Sie sich entschieden haben, `sysvinit-core` zu verwenden.

Nach dem Umstieg auf `systemd` als Standard-init-System in Jessie und weiteren Anpassungen in Stretch sind verschiedene SysV-betreffende Pakete jetzt nicht mehr erforderlich und können gefahrlos entfernt werden; verwenden Sie dazu

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

## 5.2 Einschränkungen bei der Sicherheitsunterstützung

Es gibt einige Pakete, bei denen Debian nicht versprechen kann, dass zur Behebung von Sicherheitslücken nicht minimale Rückportierungen in die Pakete mit einfließen. Diese Pakete werden in den folgenden Abschnitten behandelt.

#### ANMERKUNG



Das Paket `debian-security-support` hilft Ihnen dabei, den Sicherheitsstatus der installierten Pakete im Blick zu behalten.

### 5.2.1 Sicherheitsstatus von Webbrowsern und deren Rendering-Engines

Debian 10 enthält mehrere Browser-Engines, die einem ständigen Ansturm von Sicherheitsproblemen ausgesetzt sind. Die hohe Rate von Anfälligkeiten und die teilweise fehlende Unterstützung seitens der Originalautoren in Form von langfristig gepflegten Programmversionen machen es sehr schwierig, für

diese Browser und Engines Sicherheitsunterstützung auf Basis von rückportierten Fehlerkorrekturen anzubieten. Zusätzlich machen es Abhängigkeiten zwischen beteiligten Bibliotheken extrem schwierig, auf neuere Upstream-(Original-)Versionen hochzurüsten. Browser, die auf Engines wie „webkit“, „qtwebkit“ und „khtml“<sup>1</sup> aufbauen, sind daher in Buster zwar enthalten, es besteht jedoch für sie keine Sicherheitsunterstützung. Diese Browser sollten nicht für Verbindungen zu Websites verwendet werden, denen Sie nicht vertrauen. Das Quellpaket `webkit2gtk` ist jedoch von der Sicherheitsunterstützung abgedeckt.

Generell empfehlen wir als Webbrowser Firefox oder Chromium. Sie werden für Stable aktuell gehalten, indem Sie auf Basis der neuesten ESR-Versionen jeweils neu gebaut werden. Die gleiche Strategie wird auch für Thunderbird angewandt.

### 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 Eingriffe bei einigen spezifischen Paketen

In den meisten Fällen sollten Pakete problemlos von Stretch nach Buster aktualisiert werden. Es gibt jedoch eine kleine Anzahl von Paketen, bei denen manuelle Eingriffe erforderlich sein könnten, entweder vor oder während dem Upgrade; hier eine detaillierte Liste solcher Pakete.

### 5.3.1 Semantik für die Nutzung von Umgebungsvariablen durch `su` geändert

`su` hat mit der Version in Buster die Semantik geändert und behält nicht mehr die Umgebungsvariablen `DISPLAY` und `XAUTHORITY`. Sie müssen sie explizit setzen und so bewußt den Zugriff auf Ihr Display erlauben, wenn Sie grafische Anwendungen mit `su` nutzen möchten. Im [Fehlerbericht #905409](https://bugs.debian.org/905409) (<https://bugs.debian.org/905409>) finden Sie eine umfangreiche Diskussion zu diesem Thema.

### 5.3.2 Neuindexierung vorhandener PostgreSQL-Datenbanken erforderlich

Wenn Sie von Debian Stretch auf Buster hochrüsten, werden dabei die `glibc`-Locale-Daten aktualisiert. Im speziellen ändert sich dabei die Art, wie PostgreSQL die Daten in Text-Index-Beständen sortiert. Um Beschädigungen zu vermeiden, müssen solche Indexe mit `REINDEX` neu generiert werden, unmittelbar nachdem das `locales`- oder `locales-all`-Paket aktualisiert wurde und bevor die Datenbank zurück in den Produktionsstatus geht.

Empfohlener Befehl:

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

Alternativ können Sie die Datenbanken mit `pg_upgradecluster` auf PostgreSQL 11 hochrüsten. (Dabei wird standardmäßig `pg_dump` verwendet, was zu einer Neuindexierung aller Indexe führt. Die Verwendung von `-m upgrade` oder `pg_upgrade` ist *nicht* sicher, da dabei die jetzt inkorrekte Sortierreihenfolge erhalten bleibt.)

Lesen Sie das [PostgreSQL Wiki](https://wiki.postgresql.org/wiki/Locale_data_changes) ([https://wiki.postgresql.org/wiki/Locale\\_data\\_changes](https://wiki.postgresql.org/wiki/Locale_data_changes)), wenn Sie weitere Informationen benötigen.

### 5.3.3 `mutt` und `neomutt`

In Debian Stretch enthielt `mutt` Patches aus dem Quellcode von <https://neomutt.org> (<https://neomutt.org>). Ab Debian Buster wird das Paket, welches `/usr/bin/mutt` bereitstellt, jedoch wieder auf dem

<sup>1</sup>Diese Engines sind in einer ganzen Reihe von Quellpaketen enthalten und die aufgeführten Bedenken gelten für all diese Pakete. Sie gelten auch für solche Pakete, die die Engine enthalten, aber hier nicht explizit aufgeführt sind (mit Ausnahme von `webkit2gtk`).



reinen Mutt-Quellcode von <http://www.mutt.org> (<http://www.mutt.org>) beruhen, und ein separates `neomutt`-Paket wird zur Verfügung gestellt, welches `/usr/bin/neomutt` enthält.

Dies bedeutet, dass einige Funktionalitäten, die bisher in `mutt` enthalten waren, jetzt nicht mehr verfügbar sind. Falls dies Ihre Konfiguration unbrauchbar macht, können Sie stattdessen `neomutt` installieren.

### 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) (<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) (<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 (Abschnitt 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-permissions` 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) (<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) (<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) (<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) (<https://bugs.debian.org//802211>).



# Kapitel 6

## Zusätzliche Informationen zu Debian

### 6.1 Weitere Lektüre

Neben diesen Hinweisen zur Veröffentlichung und der Installationsanleitung sind weitere Informationen zu Debian beim Debian-Dokumentationsprojekt (DDP) erhältlich, dessen Ziel es ist, hochwertige Dokumentation für Debian-Anwender und -Entwickler zu erstellen. Dazu gehören die Debian-Referenz, der Debian-Leitfaden für neue Paketbetreuer, die häufig gestellten Fragen zu Debian (Debian-FAQ) und viele weitere. Bezüglich genauer Details über die zur Verfügung stehenden Dokumente sehen Sie auf der [Debian-Dokumentations-Website](https://www.debian.org/doc/) (<https://www.debian.org/doc/>) und im [Debian Wiki](https://wiki.debian.org/) (<https://wiki.debian.org/>) nach.

Dokumentation zu einzelnen Paketen ist in `/usr/share/doc/Paket` installiert. Das schließt Urheberrechtsinformationen, Debian-spezifische Details und Dokumentation der Original-Autoren ein.

### 6.2 Hilfe bekommen

Es gibt viele Quellen für Hilfe, Ratschläge und Unterstützung für Debian-Anwender, aber sie sollten möglichst nur in Betracht gezogen werden, wenn Sie die vorhandene Dokumentation nach Lösungen für Ihr Problem durchsucht haben. Dieser Abschnitt gibt eine kurze Einführung zu diesen Quellen, die besonders für neue Debian-Anwender hilfreich sein werden.

#### 6.2.1 Mailinglisten

Die für Debian-Anwender interessantesten Mailinglisten sind „debian-user“ (Englisch) und weitere, wie `debian-user-sprache` (für verschiedene Sprachen, bspw. `debian-user-german`). Weitere Informationen zu den Listen und wie diese abonniert werden können, sind auf den Seiten der [Debian-Mailinglisten](https://lists.debian.org/) (<https://lists.debian.org/>) beschrieben. Bitte suchen Sie vor dem Schreiben erst in den Listenarchiven nach bereits gegebenen Antworten und bitte beachten Sie auch die Etikette für die Kommunikation auf Mailinglisten.

#### 6.2.2 Internet Relay Chat

Debian hat einen IRC-Kanal im OFTC-IRC-Netzwerk, der für die Unterstützung von Debian-Anwendern bestimmt ist. Um in diesen Kanal zu gelangen, verbinden Sie Ihr IRC-Programm mit `irc.debian.org` und verwenden Sie den Kanal `#debian` (englisch).

Bitte beachten Sie die Leitsätze im Umgang mit dem Kanal und respektieren Sie die anderen Benutzer. Die Leitsätze finden Sie im [Debian Wiki](https://wiki.debian.org/DebianIRC) (<https://wiki.debian.org/DebianIRC>).

Für weitere Informationen zum OFTC besuchen Sie bitte dessen [Website](http://www.oftc.net/) (<http://www.oftc.net/>).

### 6.3 Fehler berichten

Wir bemühen uns, Debian zu einem hochqualitativen Betriebssystem zu machen. Das bedeutet aber nicht, dass alle Pakete, die wir zur Verfügung stellen, fehlerfrei sind. Übereinstimmend mit Debians

Philosophie der „offenen Entwicklung“ und als Service für unsere Anwender stellen wir alle Informationen zu gemeldeten Fehlern in unserer Fehlerdatenbank (Bug Tracking System, BTS) bereit. Dieses BTS können Sie unter <https://bugs.debian.org/> durchsuchen.

Falls Sie einen Fehler in der Distribution oder einem darin enthaltenen Paket finden, berichten Sie den Fehler bitte, sodass er für weitere Veröffentlichungen ordentlich behoben werden kann. Um Fehler zu berichten, ist eine gültige E-Mail-Adresse nötig. Wir bitten darum, damit wir Fehler verfolgen und die Entwickler Kontakt zu denjenigen aufnehmen können, die den Fehler berichtet haben, wenn weitere Informationen dazu benötigt werden.

Sie können einen Fehler mit Hilfe des Programms **reportbug** oder manuell per E-Mail berichten. Weitere Informationen zum Fehlerdatenbanksystem und wie es zu bedienen ist finden Sie in der Referenzdokumentation (unter `/usr/share/doc/debian`, wenn Sie `doc-debian` installiert haben) oder online in der **Fehlerdatenbank** (<https://bugs.debian.org/>).

## 6.4 Zu Debian beitragen

Sie müssen kein Experte sein, um etwas zu Debian beitragen zu können. Sie unterstützen die Gemeinschaft beispielsweise, indem Sie bei den verschiedenen Benutzeranfragen in den **User-Mailinglisten** (<https://lists.debian.org/>) helfen. Fehler im Zusammenhang mit der Entwicklung der Distribution zu finden (und zu beheben), indem Sie sich in den **Entwickler-Mailinglisten** (<https://lists.debian.org/>) einbringen, ist ebenfalls sehr hilfreich. Sie helfen Debians hochqualitativer Distribution auch, indem Sie **Fehler berichten** (<https://bugs.debian.org/>) und die Entwicklern dabei unterstützen, diese genauer zu identifizieren und zu lösen. Das Programm `how-can-i-help` hilft Ihnen dabei, passende Fehlerberichte zu finden, an denen Sie arbeiten können. Falls Sie gut im Umgang mit Worten sind, können Sie auch helfen, **Dokumentation** (<https://www.debian.org/doc/vcs>) zu schreiben oder bereits bestehende Dokumentation in Ihre eigene Sprache zu **übersetzen** (<https://www.debian.org/international/>).

Falls Sie mehr Zeit zur Verfügung haben, könnten Sie auch einen Teil der Freien Software in Debian verwalten. Besonders hilfreich ist es, wenn Teile übernommen werden, für die darum gebeten wurde, sie Debian zu hinzuzufügen. Die **Datenbank der Arbeit bedürftigen Pakete (WNPP)** (<https://www.debian.org/devel/wnpp/>) gibt dazu detaillierte Informationen. Falls Sie Interesse an bestimmten Anwendergruppen haben, finden Sie vielleicht Freude daran, etwas zu einzelnen **Unterprojekten** (<https://www.debian.org/devel/#projects>) von Debian beizutragen, wie beispielsweise zur Portierung auf andere Architekturen und zu **Debian Pure Blends** (<https://wiki.debian.org/DebianPureBlends>) (angepasste Debian-Distributionen).

Ob Sie nun als Anwender, Programmierer, Autor oder Übersetzer in der Gemeinschaft der Freien Software arbeiten, Sie helfen auf jeden Fall den Bemühungen der Freie-Software-Bewegung. Mitzuhelfen macht Spaß und honoriert die Arbeit anderer, und genauso wie es Ihnen ermöglicht, neue Leute kennen zu lernen, gibt es Ihnen auch dieses unbestimmte, schöne Gefühl, dabei zu sein.

# Kapitel 7

## Glossar

### **ACPI**

Advanced Configuration and Power Interface

### **ALSA**

Advanced Linux Sound Architecture

### **BD**

Blu-ray Disc

### **CD**

Compact Disc

### **CD-ROM**

Compact Disc Read Only Memory

### **DHCP**

Dynamic Host Configuration Protocol

### **DLBD**

Dual Layer (doppellagige) Blu-ray Disc

### **DNS**

Domain Name System

### **DVD**

Digital Versatile Disc

### **GIMP**

GNU Image Manipulation Program

### **GNU**

GNU's Not Unix

### **GPG**

GNU Privacy Guard

### **LDAP**

Lightweight Directory Access Protocol

### **LSB**

Linux Standard Base

### **LVM**

Logical Volume Manager

### **MTA**

Mail Transport Agent

**NBD**

Network Block Device

**NFS**

Network File System

**NIC**

Network Interface Card

**NIS**

Network Information Service

**PHP**

PHP: Hypertext Preprocessor

**RAID**

Redundanz-Array für voneinander unabhängige Platten

**SATA**

Serial Advanced Technology Attachment

**SSL**

Secure Sockets Layer

**TLS**

Transport Layer Security

**UEFI**

Unified Extensible Firmware Interface

**USB**

Universal Serial Bus

**UUID**

Universally Unique Identifier

**WPA**

Wi-Fi Protected Access

## Anhang A

# Verwalten Ihres Stretch-Systems vor dem Upgrade

Dieser Anhang enthält Informationen darüber, wie Sie sicherstellen, dass Sie ein Upgrade von Paketen aus Stretch durchführen oder diese installieren können, bevor Sie das Upgrade auf Buster durchführen. Dies sollte nur in besonderen Situationen notwendig sein.

### A.1 Upgrade Ihres Stretch-Systems

Dem Grunde nach ist dies nichts anderes als jedes bisherige Upgrade von Stretch. Der einzige Unterschied besteht darin, dass Sie zuerst sicherstellen müssen, dass Ihre Paketliste noch Referenzen für stretch enthält, wie es in Abschnitt [A.2](#) erklärt ist.

Falls Sie zum Upgrade Ihres Systems einen Debian-Spiegel nutzen, so erfolgt das Upgrade automatisch auf die neueste Zwischenveröffentlichung (sogenanntes Point-Release) von Stretch.

### A.2 Überprüfen Ihrer Paketquellen (APT source-list-Dateien)

Falls sich Zeilen in Ihren APT source-list-Dateien (siehe [sources.list\(5\)](#) (<https://manpages.debian.org/buster//buster/apt/sources.list.5.html>)) auf „stable“ beziehen, zeigen sie effektiv schon auf Buster-Paketquellen. Dies ist möglicherweise nicht das, was Sie möchten, falls Sie noch nicht bereit für das Upgrade sind. Wenn Sie bereits **apt update** ausgeführt haben, können Sie ohne Probleme mit der unten aufgeführten Anweisung wieder auf den alten Zustand zurückkehren.

Falls Sie bereits Pakete aus Buster installiert haben, ergibt es wahrscheinlich keinen Sinn mehr, Pakete aus Stretch zu installieren. In diesem Fall müssen Sie selbst entscheiden, ob Sie fortfahren wollen oder nicht. Es besteht die Möglichkeit, zu alten Paketversionen zurückzukehren, dies wird hier aber nicht beschrieben.

Öffnen Sie als `root` die entsprechende source-list-Datei mit einem Editor und überprüfen Sie alle Zeilen, die mit `deb http:`, `deb https:`, `deb tor+http:`, `deb tor+https:`, `URIs: http:`, `URIs: https:`, `URIs: tor+http:` oder `URIs: tor+https:` beginnen, ob sie Referenzen auf „stable“ enthalten. Falls ja, ändern Sie diese von `stable` in `stretch`.

Falls Zeilen vorkommen, die mit `deb file:` oder `URIs: file:` beginnen, müssen Sie selbst überprüfen, ob der darin angegebene Ort ein Archiv von Stretch oder Buster enthält.

#### WICHTIG



Ändern Sie keine Zeilen, die mit `deb cdrom:` oder `URIs: cdrom:` beginnen. Dies würde dazu führen, dass die Zeile ungültig wird und Sie **apt-cdrom** erneut ausführen müssen. Es ist kein Problem, falls eine „cdrom“-Quellzeile „unstable“ enthält. Dies ist zwar verwirrend, aber normal.

Falls Sie Änderungen vorgenommen haben, speichern Sie die Datei und führen Sie

```
# apt update
```

aus, um die Paketliste neu einzulesen.

### A.3 Veraltete Konfigurationsdateien entfernen

Bevor Sie Ihr System auf Buster aktualisieren, wird empfohlen, alte Konfigurationsdateien (wie \*.dpkg-{new,old}-Dateien in /etc) vom System zu entfernen.

### A.4 Upgrade von veralteten Gebietsschemata (Locales) auf UTF-8

Die Verwendung einer nicht-UTF-8-Locale wird seit langer Zeit von Desktop-Umgebungen und anderen Mainstream-Software-Projekten nicht mehr unterstützt. Solche Locales sollten aktualisiert werden, indem Sie **dpkg-reconfigure locales** ausführen und dort eine UTF-8-Locale auswählen. Sie sollten auch sicherstellen, dass Benutzer die Standardeinstellung nicht überschreiben, um trotzdem eine alte Locale zu verwenden.

## Anhang B

# Mitwirkende bei den Veröffentlichungshinweisen

Viele Leute haben bei den Veröffentlichungshinweisen mitgeholfen. Dazu gehören unter anderen:

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 und W. Martin Borgert.

Dieses Dokument wurde in viele Sprachen übersetzt. Vielen Dank an die Übersetzer!

Deutsche Übersetzung von: Holger Wansing.





# Index

## A

Apache, 4

## B

BIND, 4

## C

Calligra, 3

Cryptsetup, 4

## D

DocBook XML, 2

Dovecot, 4

## E

Evolution, 4

Exim, 4

## G

GCC, 4

GIMP, 4

GNOME, 3

GNUCash, 3

GnuPG, 4

## I

Inkscape, 4

## K

KDE, 3

## L

LibreOffice, 3

LXDE, 3

LXQt, 3

## M

MariaDB, 4

MATE, 3

## N

Nginx, 4

## O

OpenJDK, 4

OpenSSH, 4

## P

packages

  apparmor, 5

  apparmor-profiles-extra, 5

  apt, 2, 15, 16

  apt-listchanges, 21

  aptitude, 14, 19, 24

  cryptsetup, 6

  cups, 7

  cups-browsed, 7

  cups-filters, 6

  dblatex, 2

  debian-goodies, 19

  debian-kernel-handbook, 24

  debian-security-support, 31

  dkim-milter-python, 31

  dkimpy-milter, 31

  doc-debian, 36

  docbook-xsl, 2

  dpkg, 2

  ecryptfs-utils, 30

  evince, 5

  evolution, 33

  evolution-ews, 33

  fcitx, 30

  gnome-control-center, 33

  gnome-disk-utility, 33

  grub-efi-amd64-signed, 4

  grub-efi-ia32-signed, 4

  haveged, 28

  how-can-i-help, 36

  icinga, 30

  icinga2, 30

  icinga2-classicui, 30

  icingaweb2, 30

  ifupdown, 28

  initramfs-tools, 12, 23

  ipsec-tools, 30

  iptables, 5

  keepass2, 30

  libreswan, 30

  linux-image-\*, 23

  linux-image-amd64, 23

  linux-source, 24

  localepurge, 20

  locales, 32

  locales-all, 32

  mailman, 31

  mailman3, 30

  mailman3-full, 30

  manpages-de, 5

  mcelog, 30

  mutt, 5, 32, 33

  neomutt, 33

  phpmyadmin, 30

  popularity-contest, 19

  pyspf-milter, 31

  python-2.7, 30

  raccoon, 30

  rasdaemon, 30

  release-notes, 1

  Revelation, 30

  revelation, 30

  rpcbind, 27

  s3ql, 33

  shim-signed, 4

  spf-milter-python, 31

  sshd, 27

---

ssmtp, 30  
synaptic, 14, 30  
systemd, 5, 28, 29  
tinc, 13  
udev, 23, 28  
unattended-upgrades, 5  
upgrade-reports, 2  
usrmerge, 7  
util-linux, 5  
xmlroff, 2  
xsltproc, 2  
ypbind, 27  
Perl, 4  
PHP, 4  
Postfix, 4  
PostgreSQL, 4

**X**  
Xfce, 3