Hinweise zur Debian-Veröffentlichung Version 11 (Bullseye) auf ARM EABI

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

26. Juni 2022

Inhaltsverzeichnis

Kapitel 1

Einführung

Dieses Dokument informiert Benutzer der Debian-Distribution über entscheidende Änderungen in Version 11 (Codename Bullseye).

Die Hinweise zur Veröffentlichung enthalten Informationen, wie ein sicheres Upgrade von Version 10 (Codename Buster) 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/bullseye/releasenotes`.

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 Buster) 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 Buster 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/`). Sie können auch zunächst die bereits vorhandenen Fehlerberichte (`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 Buster auf Bullseye 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 11

Das Wiki (`https://wiki.debian.org/NewInBullseye`) enthält weitere Informationen zu diesem Thema.

2.1 Unterstützte Architekturen

Die folgenden Architekturen werden offiziell von Debian 11 unterstützt:

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

Näheres zum Stand der Portierungen und Port-spezifische Informationen für Ihre Architektur finden Sie auf Debians Portierungs-Webseiten (`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 Buster; die Distribution enthält über 11294 neue Pakete und damit insgesamt über 59551 Pakete. Ein Großteil der Software in der Distribution wurde aktualisiert: über 42821 Softwarepakete (das entspricht 72% aller Pakete in Buster). Außerdem wurde eine signifikante Zahl von Paketen (über 9519, 16% der Pakete in Buster) 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.

2.2.1 Desktop-Umgebungen und bekannte Pakete

Debian erscheint wieder mit verschiedenen Desktop-Anwendungen und -Umgebungen. Unter anderem enthält es die Desktop-Umgebungen GNOME 3.38, KDE Plasma 5.20, LXDE 11, LXQt 0.16, MATE 1.24 und Xfce 4.16.

Produktivprogramme wurden ebenfalls aktualisiert, inklusive der Büroanwendungs-Pakete:

- LibreOffice wurde auf Version 7.0 aktualisiert;
- Calligra wurde auf Version 3.2 aktualisiert.

- GNUcash wurde auf Version 4.4 aktualisiert;

Neben vielen weiteren enthält diese Veröffentlichung auch folgende Aktualisierungen:

Paket	Version in 10 (Buster)	Version in 11 (Bullseye)
Apache	2.4.38	2.4.48
BIND - DNS-Server	9.11	9.16
Cryptsetup	2.1	2.3
Dovecot - MTA	2.3.4	2.3.13
Emacs	26.1	27.1
Exim - Standard-E-Mail-Server	4.92	4.94
GNU Compiler Collection als Standard-Kompiliersoftware	8.3	10.2
GIMP	2.10.8	2.10.22
GnuPG	2.2.12	2.2.27
Inkscape	0.92.4	1.0.2
GNU-C-Bibliothek	2.28	2.31
lighttpd	1.4.53	1.4.59
Linux-Kernel-Image	4.19-Serie	5.10-Serie
LLVM/Clang-Werkzeugkette	6.0.1 und 7.0.1 (Standardversion)	9.0.1 und 11.0.1 (Standardversion)
MariaDB	10.3	10.5
Nginx	1.14	1.18
OpenJDK	11	11
OpenSSH	7.9p1	8.4p1
Perl	5.28	5.32
PHP	7.3	7.4
Postfix - MTA	3.4	3.5
PostgreSQL	11	13
Python 3	3.7.3	3.9.1
Rustc	1.41 (1.34 für `armel`)	1.48
Samba	4.9	4.13
Vim	8.1	8.2

2.2.2 Treiberloses Scannen und Drucken

Sowohl das Drucken mit `CUPS` wie auch Scannen mit `SANE` funktioniert in zunehmendem Maße (speziell bei Geräten, die ca. in den letzten 5 Jahren auf den Markt gekommen sind) ohne die Installation von oft nicht-freien und für das Gerätemodell spezifischen Treibern.

2.2.2.1 CUPS und treiberloses Drucken

Moderne Drucker, die über Ethernet oder WLAN verbunden sind, können bereits treiberloses Drucken (`https://wiki.debian.org/CUPSQuickPrintQueues`) verwenden, implementiert über `CUPS` und `cups-filters`; dies ist bereits in den Veröffentlichungshinweisen für Buster (`https://www.debian.org/releases/buster/amd64/release-notes/ch-whats-new.html#driverless-printing`) beschrieben. Debian 11 „Bullseye“ bringt das neue Paket `ipp-usb` mit, das von `cups-daemon` empfohlen wird, und nutzt das herstellerneutrale IPP-over-USB (`https://wiki.debian.org/CUPSDriverlessPrinting#ippoverusb`)-Protokoll, das auch viel moderne Drucker unterstützen. Dies erlaubt es, USB-Drucker wie einen Netzwerkdrucker zu behandeln, was die Möglichkeiten des treiberlosen Druckens auf per USB angebundene Geräte ausweitet. Spezifische Details sind im Wiki (`https://wiki.debian.org/CUPSDriverlessPrinting#ipp-usb`) zusammengefasst.

Der im `ipp-usb`-Paket enthaltene systemd-Service startet den `ipp-usb`-Daemon, wenn ein Drucker über USB angeschlossen wird, und stellt ihn so für das Drucken zur Verfügung. Standardmäßig sollte der Drucker über `cups-browsed` automatisch konfiguriert werden, andernfalls kann er aber auch manuell mit einer lokalen treiberlosen Druckerwarteschlange eingerichtet werden (`https://wiki.debian.org/SystemPrinting`).

2.2.2.2 SANE und treiberloses Scannen

Das offizielle treiberlose SANE-Backend wird von sane-escl aus dem Paket libsane1 bereitgestellt. Ein weiteres, unabhängig davon entwickeltes treiberloses Backend ist sane-airscan. Beide verstehen das eSCL-Protokoll (https://wiki.debian.org/SaneOverNetwork#escl), aber sane-airscan kann zusätzlich auch das WSD-Protokoll (https://wiki.debian.org/SaneOverNetwork#wsd) nutzen. Benutzer sollten in Betracht ziehen, beide Backends auf ihrem System zu installieren.

eSCL und WSD sind Netzwerkprotokolle. Das bedeutet, dass sie über eine USB-Verbindung arbeiten, wenn der Scanner ein IPP-over-USB-Gerät ist (siehe oben). Beachten Sie, dass libsane1 die Verwendung des Pakets ipp-usb empfiehlt. Das führt dazu, dass für entsprechende Geräte automatisch die Nutzung eines treiberlosen Backends eingerichtet wird, sobald es per USB angeschlossen ist.

2.2.3 Neuer generischer open-Befehl

Der neue Befehl **open** ist jetzt als komfortable Alternative zu **xdg-open** (Standard) oder **run-mailcap** verfügbar, konfigurierbar über das update-alternatives (https://manpages.debian.org//bullseye/dpkg/update-alternatives.1.html)-System. Es ist für die interaktive Nutzung auf der Befehlszeile gedacht, um Dateien mit der zugehörigen Standardanwendung zu öffnen, welche auch ein grafisches Programm sein kann, wenn verfügbar.

2.2.4 Control groups v2

In Bullseye verwendet systemd standardmäßig control groups v2 (cgroupv2), das eine einheitliche Hierarchie zur Ressourcenkontrolle bereitstellt. Es sind Kernel-Parameter verfügbar, um - falls nötig - wieder die alte cgroups-Variante zu aktivieren; beachten Sie die Hinweise für OpenStack im Abschnitt 5.1.8-Abschnitt.

2.2.5 Dauerhaftes systemd-Journal

Systemd aktiviert in Bullseye standardmäßig die Funktion für ein dauerhaftes Journal (persistent journal), und speichert seine Log-Dateien in /var/log/journal/. Details finden Sie unter systemd-journald.service(8) (https://manpages.debian.org//bullseye/systemd/systemd-journald.service.8.html); beachten Sie, dass in Debian das Journal zusätzlich zur systemd-journal-Gruppe (Standardeinstellung) auch für Mitglieder der Gruppe adm lesbar ist.

Dies sollte nicht zu Beeinträchtigungen mit jeglichen vorhandenen traditionellen Logging-Daemons wie z.B. rsyslog führen, aber Benutzer, die nicht zwingend spezielle Funktionen eines solchen Daemons benötigen, könnten in Betracht ziehen, diesen zu deinstallieren und in Zukunft nur das Journal zu verwenden.

2.2.6 Neue Fcitx-5-Eingabemethode

Fcitx 5 ist eine Eingabemethode für Chinesisch, Koreanisch und viele andere Sprachen. Es ist der Nachfolger des beliebten Fcitx 4 in Buster. Die neue Version unterstützt Wayland und hat eine bessere Addon-Unterstützung. Weitere Informationen inklusive der Migrationsanleitung finden Sie im Wiki (https://wiki.debian.org/I18n/Fcitx5).

2.2.7 Neuigkeiten vom Debian Med Blend

Das Debian-Med-Team hat im Kampf gegen COVID-19 Software für die Virusforschung auf Sequenzierungsebene paketiert, sowie Werkzeuge, die zur Bekämpfung der Epidemie eingesetzt werden.

Neben neu hinzugefügten Paketen auf dem Feld der Biowissenschaften und Medizin haben viele vorhandene Pakete Unterstützung für Continuous Integration erfahren.

Eine Reihe performance-kritischer Anwendungen profitieren jetzt von SIMD Everywhere (https://wiki.debian.org/SIMDEverywhere). Diese Bibliothek erlaubt Paketen die Verfügbarkeit auf weiteren, von Debian unterstützten Hardware-Plattformen (vor allem arm64), unter gleichzeitiger Nutzung der Performance-Vorteile von Prozessoren, die Vektorerweiterungen bereitstellen (wie AVX auf amd64 oder NEON auf arm64).

Um Pakete zu nutzen, die vom Debian-Med-Team betreut werden, installieren Sie die Metapakete namens `med-*`, die für Debian Bullseye in der Version 3.6.x bereitstehen. Besuchen Sie gerne die Debian-Med Tasks-Seiten (`https://blends.debian.org/med/tasks`), um einen vollständigen Überblick über biologische und medizinische Software in Debian zu erhalten.

2.2.8 Kernel-Unterstützung für exFAT

Bullseye ist die erste Veröffentlichung, die einen Linux-Kernel mit Unterstützung für das exFAT-Dateisystem enthält. Diese wird auch standardmäßig für das Einbinden von exFAT-Dateisystemen verwendet. Konsequenterweise ist es daher auch nicht mehr erforderlich, die filesystem-in-userspace-Implementierung aus dem `exfat-fuse`-Paket zu verwenden. Falls Sie diese trotzdem noch weiter nutzen möchten, müssen Sie das Hilfsskript **mount.exfat-fuse** händisch aufrufen, wenn Sie ein exFAT-Dateisystem einbinden.

Werkzeuge zur Erzeugung und Überprüfung von exFAT-Dateisystemen werden von den Autoren der exFAT-Implementierung des Linux-Kernels in dem `exfatprogs`-Paket bereitgestellt. Es gibt auch noch die davon unabhängige Implementierung vergleichbarer Hilfsprogramme im `exfat-utils`-Paket, allerdings kann dieses Paket nicht parallel zu der neuen Implementierung installiert werden. Es wird empfohlen, zum `exfatprogs`-Paket zu migrieren, aber achten Sie dabei auf die Befehlsoptionen, die höchstwahrscheinlich inkompatibel zueinander sind.

2.2.9 Verbesserte Übersetzungen von Handbuchseiten

Die Handbuchseiten (manpages) für verschiedene Projekte wie systemd, util-linux, OpenSSH und Mutt wurden in mehreren Sprachen (darunter Französisch, Spanisch und Mazedonisch) wesentlich verbessert. Um hiervon zu profitieren, installieren Sie bitte `manpages-`*`xx`* (dabei ist *`xx`* der Sprachcode Ihrer bevorzugten Sprache).

Während des Lebenszyklus von Debian Bullseye werden weitere verbesserte Übersetzungen über das `backports`-Archiv bereitgestellt.

2.2.10 Verbesserte Unterstützung für alternative Init-Systeme

Das Standard-Init-System in Debian ist `systemd`. In Bullseye werden aber auch eine Reihe von alternativen Init-Systemen unterstützt (z.B. das System-V-artige Init oder OpenRC), und die meisten Arbeitsplatz-Umgebungen funktionieren jetzt auch gut auf Systemen mit alternativen Inits. Details, wie Sie das Init-System wechseln (sowie Infos, wo Sie Hilfe bekommen bei Problemen, wenn Sie ein anderes Init-System als systemd betreiben), finden Sie im Debian Wiki (`https://wiki.debian.org/Init`).

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 Bullseye finden Sie zusammen mit der Installationsanleitung auf der Debian-Webseite (`https://www.debian.org/releases/bullseye/debian-installer/`).

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

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

Beachten Sie bitte auch die Errata (`https://www.debian.org/releases/bullseye/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 10 viel entwickelt, was zu verbesserter Hardware-Unterstützung sowie einigen spannenden neuen Funktionen oder Verbesserungen führt.

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

3.1.1 Hilfe bei der Installation von Firmware

Immer öfter erfordern Peripheriegeräte, dass als Teil der Hardware-Initialisierung Firmware in das Gerät geladen wird. Um bei dieser Thematik zu helfen, wurde der Installer um eine zusätzliche Funktionalität erweitert. Über eine Zuordnung der Hardware-ID zu Firmware-Dateien wird detektiert, ob installierte Hardware Firmware erfordert. Dabei als erforderlich erkannte Firmware wird automatisch installiert.

Diese neue Funktionalität ist allerdings auf die inoffiziellen Installer-Images beschränkt, die Firmware-Dateien enthalten (siehe https://www.debian.org/releases/bullseye/debian-installer/#firmware_nonfree (`https://www.debian.org/releases/bullseye/debian-installer/#firmware_nonfree`)). Solche Firmware ist für gewöhnlich nicht DFSG-kompatibel, und kann daher nicht über Debian's Main-Archiv verteilt werden.

Falls Sie Probleme bemerken, die (fehlende) Firmware betrifft, sollten Sie das zugehörige Kapitel der Installationsanleitung (`https://www.debian.org/releases/bullseye/amd64/ch06s04#completing-ins`) lesen.

3.1.2 Automatisierte Installation

Einige der Änderungen ziehen auch Veränderungen 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 Buster funktioniert haben, nun auch mit dem neuen Installer funktionieren, zumindest nicht ohne Anpassungen.

Die Installationsanleitung (`https://www.debian.org/releases/bullseye/installmanual`) enthält einen aktualisierten Anhang mit ausführlicher Dokumentation über die Verwendung der Vorkonfiguration.

3.2 Images für Container und virtuelle Maschinen

Multi-Architektur Container-Images sind für Debian Bullseye auf Docker Hub (`https://hub.docker.com/_/debian`) verfügbar. Zusätzlich zu den Standard-Images gibt es auch eine abgespeckte „slim“-Variante, die den genutzten Festplattenplatz reduziert.

Images für virtuelle Maschinen werden für den Hashicorp Vagrant VM-Manager über die Vagrant Cloud (`https://app.vagrantup.com/debian`) bereitgestellt.

Kapitel 4

Upgrade von Debian 10 (Buster)

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 Bullseye 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 Bedienereingabe während des Prozesses erfordert[1].

Wenn das zu aktualisierende System kritische Dienste für Ihre Nutzer oder für das Netzwerk bereitstellt[2], 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 Bullseye. 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/bullseye/installmanual`) und die FAQ des Debian-Installers (`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 ein Live-Installations-Image (`https://www.debian.org/CD/live/`)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[3] 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.

[1] 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.

[2] 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.

[3] 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/`)-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.

Benutzer des watchdog-Daemons aus dem `micro-evtd`-Paket sollten den Daemon beenden und den Watchdog-Timer vor dem Upgrade deaktivieren, um einen unberechtigten Neustart während des Upgrade-Prozesses zu vermeiden:

```
# service micro-evtd stop
# /usr/sbin/microapl -a system_set_watchdog off
```

4.2 Start des Upgrades von einem „reinen“ Debian-System

Der Upgrade-Prozess, wie er in diesem Kapitel beschrieben wird, ist für „reine“ Debian Stable-Systeme konzipiert. APT steuert, was auf Ihrem System installiert ist. Falls Ihre APT-Konfiguration noch weitere Paketquellen zusätzlich zu buster 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.

Die Haupt-Konfigurationsdatei, die APT verwendet, um festzulegen, welche Paketquellen zum Download von Paketen genutzt werden, ist `/etc/apt/sources.list`, aber es können auch weitere Dateien

im Verzeichnis `/etc/apt/sources.list.d/` zum Einsatz kommen - Details hierzu finden Sie unter sources.list(5) (`https://manpages.debian.org//bullseye/apt/sources.list.5.html`). Wenn Ihr System mehrere source-list-Dateien verwendet, müssen Sie sicherstellen, dass diese untereinander konsistent sind.

4.2.1 Upgrade auf Debian 10 (Buster)

Direkte Upgrades ausgehend von Debian-Systemen älter als Version 10 (buster) werden nicht unterstützt. Sie können sich die aktuell auf Ihrem System laufende Debian-Version anzeigen lassen mit:

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

Bitte befolgen Sie die Anweisungen in den Hinweisen zur Debian-Veröffentlichung Version 10 (`https://www.debian.org/releases/buster/releasenotes`), um zunächst ein Upgrade auf Debian 10 durchzuführen.

4.2.2 Pakete entfernen, die nicht von Debian stammen

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

4.2.3 Upgrade auf die letzte Zwischenveröffentlichung

Diese Anleitung geht davon aus, dass Sie Ihr System auf die neueste Zwischenveröffentlichung von Buster aktualisiert haben. Falls dies nicht der Fall sein sollte oder Sie sich unsicher sind, folgen Sie den Anweisungen in Abschnitt A.1.

4.2.4 Vorbereiten der Paketdatenbank

Bevor Sie das Upgrade starten, sollten Sie kontrollieren, ob noch ausstehende Aktionen in der Paketdatenbank existieren. Falls Sie einen Paketmanager wie `aptitude` oder `synaptic` verwenden, kontrollieren Sie, ob es dort noch ausstehende Aktionen gibt. Ein Paket, das im Paketmanager zum Entfernen oder Aktualisieren vorgemerkt ist, könnte den Upgrade-Prozess negativ beeinflussen. Beachten Sie, dass Sie eine solche Situation nur korrigieren können, solange Ihre APT source-list-Dateien noch auf *buster* verweisen und nicht auf *stable* oder *bullseye*; Näheres dazu in Abschnitt A.2.

4.2.5 Veraltete Pakete entfernen

Es ist eine gute Idee, veraltete Pakete vor dem Upgrade zu entfernen. Sie könnten sonst zu Komplikationen während des Upgrade-Prozesses führen oder ein Sicherheitsrisiko darstellen, da sie nicht mehr betreut werden.

4.2.6 Bereinigen alter Konfigurationsdateien

Von einem früheren Upgrade könnten noch ungenutzte Kopien von Konfigurationsdateien zurückgeblieben sein: alte Versionen dieser Dateien, oder Versionen, die vom Paketbetreuer bereitgestellt wurden, etc. Solche Hinterlassenschaften zu beseitigen kann Komplikationen vermeiden. Sie können solche Dateien finden mit:

```
# find /etc -name '*.dpkg-*' -o -name '*.ucf-*' -o -name '*.merge-error'
```

4.2.7 Der Bereich für Sicherheitsaktualisierungen (Security)

Für APT-source-Zeilen, die auf das Security-Archiv verweisen, hat sich das Format zusätzlich zum Release-Namen geringfügig geändert: von `buster/updates` nach `bullseye-security`. Siehe Abschnitt 5.1.2.

4.2.8 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.

4.2.9 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 Bullseye übersetzte Pakete anbietet und den Eintrag gleichzeitig mit dem für die Original-Debian-Pakete ändern.

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

4.2.10 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/`) ändern, um das Upgrade der Pakete aus der neuen Stable-Veröffentlichung zu erlauben. Weitere Informationen zu APT Pinning finden Sie unter apt_preferences(5) (`https://manpages.debian.org//bullseye/apt/apt_preferences.5.en.html`).

4.2.11 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
```

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:

[4] 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.

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

Um Pakete, die für **apt** auf hold gesetzt wurden, 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 buster 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: Zeilen für `bullseye` müssen hinzugefügt und solche für `buster` üblicherweise entfernt werden.

`apt` wird alle Pakete berücksichtigen, die über die konfigurierten Paketquellen gefunden werden, und jeweils 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 über ihren Codenamen (z.B. `buster`, `bullseye`) als auch über den Statusnamen (d.h. `oldstable`, `stable`, `testing`, `unstable`) angegeben werden. Die Verwendung des Codenamens hat den Vorteil, dass Sie nie von einer neueren Veröffentlichung 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 Paketaktualisierungen 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/`) abonnieren, bekommen Sie eine Informations-Mail, wenn Debian eine neue Veröffentlichung freigibt (wenn also z.B. `Bullseye` von `testing` in `stable` überführt wird).
- Über die Debian Security-Announcement-Mailingliste (`https://lists.debian.org/debian-security-annou` erhalten Sie E-Mails, immer wenn Debian Sicherheitsankündigungen veröffentlicht.

4.3.1 APT-Internet-Quellen hinzufügen

Bei Neuinstallationen ist es mittlerweile 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 bullseye 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 eine solche Art der Konfiguration aber nach wie vor 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/bullseye/main/binary-armel/...
http://mirrors.kernel.org/debian/dists/bullseye/contrib/binary-armel/...
```

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

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

```
deb file:/var/local/debian bullseye 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 „`bullseye`“ oder auf „`stable`“ verweisen. Es sollte keine Quelleinträge für „`buster`“ 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 etwas wie

```
# script -t 2>~/upgrade-bullseye-schritt1.time -a ~/upgrade-bullseye-schritt1. ↩
    script
```

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-bullseye.script`, um die Datei durchzuschauen.

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

apt führt Protokoll über geänderten Paketstatus und speichert dies in `/var/log/apt/history.log`; außerdem wird die Terminal-Ausgabe in `/var/log/apt/term.log` abgelegt. **dpkg** wird zusätzlich Informationen über geänderten Paketstatus in `/var/log/dpkg.log` abspeichern. Wenn Sie **aptitude** benutzen, werden Statusänderungen in `/var/log/aptitude` abgelegt.

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

```
# scriptreplay ~/upgrade-bullseyeschritt.time ~/upgrade-bullseyeschritt.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

Nutzer von apt-secure könnten Probleme bekommen, wenn sie **aptitude** oder **apt-get** benutzen. Im Falle von apt-get können Sie dann **apt-get update --allow-releaseinfo-change** verwenden.

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 Buster 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 **deborphan**, **debfoster** oder **cruft** 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 **l** 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 Lokalisierungsdateien 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 /var/cache/apt/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 buster zu ändern (wie in Abschnitt A.2 beschrieben), um Pakete sicher entfernen zu können.

4.4.4 Minimales System-Upgrade

> **WICHTIG**
>
> 
>
> Falls Sie das Upgrade über eine Remote-Verbindung von fern durchführen, beachten Sie Abschnitt 5.1.22.

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 zweiteiligen 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 upgrade --without-new-pkgs
```

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 Bullseye 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 buster- wie auch bullseye-Quellen in Ihren APT source-list-Dateien anzugeben und danach **apt update** auszuführen.

4.5.2 Zu erwartende Paketentfernungen

Der Upgrade-Prozess auf Bullseye könnte auch das Entfernen von Paketen im System bedeuten. Die exakte Liste der zu entfernenden Pakete varriert 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 Bullseye 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“ Buster-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

Wenn Sie das Upgrade von der lokalen Systemkonsole aus durchführen, werden Sie vielleicht feststellen, dass in einigen Situationen die Anzeige auf eine andere Konsole umgeschaltet wird, so dass Sie den Status des Upgrade-Prozesses nicht mehr beobachten können. Zum Beispiel könnte dies auf Systemen mit grafischer Oberfläche passieren, wenn der Displaymanager neu gestartet wird.

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 Buster auf Bullseye 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
```

Falls Sie bei der Entscheidung, welches Paket Sie wählen sollen, unsicher sind, führen Sie `uname -r` aus und suchen Sie nach einem Paket mit einem ähnlichen Namen. Falls die Anzeige zum Beispiel „`4.9.0-8-amd64`“ ist, wird empfohlen, dass Sie `linux-image-amd64` installieren. Sie können auch **apt** benutzen, um eine ausführliche Beschreibung jedes Pakets zu bekommen, was Ihnen bei der Paketauswahl helfen kann. Zum Beispiel:

```
# 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 5.1.24, 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/`), 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 Buster) 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 Bullseye werden viele neue Pakete eingeführt, jedoch werden auch einige alte Pakete, die in Buster noch existierten, ausgelassen oder wegfallen. 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 Bullseye einstellen[5] 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 Bullseye angesehen. Im letzten Fall könnten sie trotzdem noch in der „unstable“-Distribution vorhanden sein.

Einige Paketmanagement-Programme bieten eine einfache Möglichkeit, um installierte Pakete zu finden, die in keinem bekannten Paketdepot mehr verfügbar sind. In der Textoberfläche von **aptitude** z.B. sind sie unter „Veraltete und selbst erstellte Pakete“ (bzw. „Obsolete and Locally Created Packages“ in Englisch) zu finden und können dort auch entfernt werden mittels:

```
# 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 Bullseye finden Sie unter Abschnitt 5.3.1.

4.8.1 Übergangs-Dummy-Pakete

Einige Pakete aus Buster könnten in Bullseye 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.

[5] 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 Bullseye 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 Bullseye

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

5.1.1 Das XFS-Dateisystem unterstützt nicht mehr die Optionen barrier/nobarrier

Die Unterstützung für die mount-Optionen `barrier` und `nobarrier` wurde aus dem XFS-Dateisystem entfernt. Es wird empfohlen, zu überprüfen, ob diese Optionen in `/etc/fstab` enthalten sind, und sie in diesem Fall zu entfernen. Bei Partitionen, für die diese Optionen verwendet werden, wird das Einbinden (mount) fehlschlagen.

5.1.2 Geändertes Layout im Security-Archiv

Für Bullseye ist die Security-Suite des Archivs jetzt mit `bullseye-security` benannt (statt dem früheren *codename*`/updates`; Benutzer sollten ihre APT source-list-Dateien beim Upgrade entsprechend anpassen.

Die Security-Zeile in Ihrer APT-Konfiguration könnte für Bullseye so aussehen:

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

Falls Ihr APT-Konfiguration auch Pinning oder `APT::Default-Release` enthält, sind dabei wahrscheinlich Anpassungen erforderlich, da der Codename im Security-Archiv nicht mehr mit dem im regulären Archiv übereinstimmt. Ein Beispiel für eine funktionierende `APT::Default-Release`-Zeile für Bullseye sieht aus wie folgt:

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

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

5.1.3 Passwort-Hash verwendet standardmäßig yescrypt

Der Passwort-Hash für lokale Systemkonten wurde geändert (`https://tracker.debian.org/news/1226655/accepted-pam-140-3-source-into-unstable/`) und nutzt standardmäßig statt SHA-512 jetzt yescrypt (`https://www.openwall.com/yescrypt/`) (nähere Infos unter crypt(5) (`https:`

//manpages.debian.org//bullseye/libcrypt-dev/crypt.5.html)). Wir erwarten, dass dies die Sicherheit gegen wörterbuchbasierte Angriffe zum Erraten von Passwörter erhöht (sowohl was den benötigten Speicher wie auch die für solch einen Angriff nötige Zeit anbetrifft).

Um von diesem Sicherheitsvorteil zu profitieren, sollten Sie Ihre lokalen Passwörter ändern, z.B. mit dem **passwd**-Befehl.

Alte Passwörter werden weiter funktionieren, unabhängig davon, welcher Passwort-Hash zu deren Erstellung verwendet wurde.

Yescrypt wird nicht von Debian 10 (Buster) unterstützt. Aufgrunddessen können shadow-Passwortdateien (`/etc/shadow`) nicht von einem Bullseye-System zurück auf ein Buster-System kopiert werden. In einem solchen Fall würden Passwörter, die unter Bullseye erstellt wurden, unter Buster nicht funktionieren. Vergleichbar dazu können Passwörter auch nicht via Kopieren&Einfügen von einem Bullseye- auf ein Buster-System übertragen werden.

Falls solch eine Kompatibilität zwischen Bullseye und Buster benötigt wird, müssen Sie `/etc/pam.d/common-password` anpassen. Suchen Sie die folgende Zeile:

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

und ersetzen Sie `yescrypt` durch `sha512`.

5.1.4 NSS-, NIS- und NIS+-Unterstützung benötigt neue Pakete

Die Unterstützung für NSS, NIS und NIS+ wurde in separate Pakete namens `libnss-nis` bzw. `libnss-nisplus` verschoben. Unglücklicherweise kann bei `glibc` keine Abhängigkeit auf diese neuen Pakete festgelegt werden, sie werden jetzt von `glibc` lediglich empfohlen.

Auf Systemen, die NIS oder NIS+ verwenden, sollte daher nach dem Upgrade kontrolliert werden, ob diese Pakete korrekt installiert sind.

5.1.5 Behandlung von Konfigurationsdatei-Fragmenten in unbound

Der DNS-Resolver `unbound` hat die Art geändert, wie mit Konfigurationsdatei-Fragmenten umgegangen wird. Falls Sie `include:`-Regeln verwenden, um einzelne Fragmente in eine gültige Konfiguration zusammenzuführen, sollten Sie die NEWS-Datei (`https://sources.debian.org/src/unbound/bullseye/debian/NEWS/`) lesen.

5.1.6 Missbilligung einiger rsync-Parameter

Die `rsync`-Parameter `--copy-devices` und `--noatime` wurden in `--write-devices` und `--open-noatime` umbenannt. Die alten Formen werden nicht mehr unterstützt; falls Sie sie verwenden, sollten Sie die NEWS-Datei (`https://sources.debian.org/src/rsync/bullseye/debian/rsync.NEWS/`) lesen. Damit Transferprozesse zwischen Systemen mit unterschiedlichen Debian-Versionen (Bullseye und Buster) funktionieren, könnte es nötig sein, die Buster-Seite auf die `rsync`-Version aus dem backports (`https://backports.debian.org/`)-Repository hochzurüsten.

5.1.7 Behandlung von Addons in vim

Die Addons für `vim`, bereitgestellt vom Paket `vim-scripts`, werden jetzt von vim's nativer „package"-Funktionalität verwaltet, statt von `vim-addon-manager`. Vim-Benutzer sollten sich vor dem Upgrade darauf vorbereiten, Instruktionen dazu sind in der NEWS-Datei (`https://sources.debian.org/src/vim-scripts/bullseye/debian/NEWS/`) zu finden.

5.1.8 OpenStack und cgroups v1

OpenStack Victoria (enthalten in Bullseye) erfordert cgroup v1 für die Block-Device QoS-Funktionalität. Da seit Bullseye die Verwendung von cgroupv2 das Standardverhalten ist (Näheres in Abschnitt 2.2.4), enthält der sysfs-Verzeichnisbaum in `/sys/fs/cgroup` keine cgroupv1-Funktionen wie `/sys/fs/cgroup/blkio`, und aufgrunddessen wird **cgcreate -g blkio:foo** fehlschlagen. Für OpenStack-Nodes, auf denen `nova-compute` oder `cinder-volume` läuft, wird dringend empfohlen, die Parameter `systemd.unified_cgro`

und `systemd.legacy_systemd_cgroup_controller=false` zur Kernel-Befehlszeile hinzuzufügen, um die Standardeinstellungen zu überschreiben und die alte cgroup-Hierarchie weiter zu verwenden.

5.1.9 OpenStack API: Regel-Dateien

Gemäß den Empfehlungen von Upstream wurde die OpenStack API von OpenStack Victoria (die in Bullseye enthaltene Version) dahingehend geändert, dass jetzt für Regel-Dateien das neue YAML-Format verwendet wird. Aufgrunddessen scheinen die meisten OpenStack-Dienste (inklusive Nova, Glance und Keystone) beschädigt zu sein, wenn die API-Regeln explizit in `policy.json`-Dateien definiert sind. Daher enthalten die Pakete jetzt ein Verzeichnis `/etc/PROJEKTNAME/policy.d` mit einer Datei namens `00_default_policy.yaml`, die alle Regeln als (standardmäßig) auskommentierte Zeilen enthält.

Um zu vermeiden, dass die alten `policy.json`-Dateien aktiv bleiben, benennen Debian's OpenStack-Pakete diese Datei jetzt um in `disabled.policy.json.old`. In einigen Fällen, für die zeitnah keine bessere Lösung gefunden werden konnte, wird die `policy.json` sogar einfach gelöscht. Es wird daher dringend empfohlen, dass Sie vor dem Upgrade Sicherungen der `policy.json`-Dateien auf Ihrem System erstellen.

Weitere Details finden Sie in der Upstream-Dokumentation (`https://governance.openstack.org/tc/goals/selected/wallaby/migrate-policy-format-from-json-to-yaml.html`).

5.1.10 sendmail nicht verfügbar während des Upgrades

Anders als bei normalen Aktualisierungen von `sendmail` wird während des Upgrades von Buster auf Bullseye der sendmail-Dienst für eine längere Zeit als gewöhnlich gestoppt. Grundsätzliche Informationen, wie Sie diese Downtime reduzieren können, finden Sie in Abschnitt 4.1.3.

5.1.11 FUSE 3

Einige Pakete wie `gvfs-fuse`, `kio-fuse` und `sshfs` haben auf FUSE 3 umgestellt. Das führt dazu, dass bei diesem Upgrade `fuse3` installiert und `fuse` vom System entfernt wird.

Unter besonderen Umständen, z.B. wenn Sie das Upgrade einfach nur durch Ausführen von **apt-get dist-upgrade** durchführen, statt durch die in Kapitel 4 dokumentierte Vorgehensweise, könnten Pakete, die von `fuse3` abhängen, zurückgehalten werden. Sie können dies Problem beheben, indem Sie die Schritte in Abschnitt 4.4.5 mit der `apt`-Version aus Bullseye erneut ausführen oder indem Sie die Pakete händisch aktualisieren.

5.1.12 GnuPG options-Datei

Beginnend mit Version 2.2.27-1 wurde die benutzerspezifische Konfiguration der `GnuPG`-Suite vollständig auf `~/.gnupg/gpg.conf` umgestellt; die Datei `~/.gnupg/options` wird nicht mehr verwendet. Bitte benennen Sie die Datei - falls notwendig - um, oder verschieben Sie deren Inhalt an den neuen Ort.

5.1.13 Linux aktiviert standardmäßig User Namespaces

Ab `Linux` 5.10 sind alle Benutzer standardmäßig berechtigt, nutzerspezifische Namensräume (User Namespaces) anzulegen. Dies erlaubt es Programmen wie Webbrowsern oder Container-Managern, restriktivere Sandbox-Umgebungen für nicht oder weniger vertrauenswürdigen Code zu erzeugen, ohne dass sie dabei als root laufen oder ein setuid-root-Hilfsskript verwenden müssen.

Früher war Debians Standardeinstellung hierbei, diese Funktionalität nur Prozessen zu erlauben, die als root laufen, weil sie weitere Sicherheitsprobleme im Linux-Kernel freigelegt hat. Da die Implementierung dieser Funktion in der Zwischenzeit aber ausgereift ist, sind wir jetzt zuversichtlich, dass das Risiko der allgemeinen Freigabe aufgewogen wird durch den Sicherheitsgewinn, den diese Funktionalität bietet.

Falls Sie es vorziehen, diese Funktion nur auf root beschränkt zu halten, setzen Sie dieses sysctl:

```
user.max_user_namespaces = 0
```

Beachten Sie aber, dass verschiedene Desktop- und Containerfunktionalitäten nicht funktionieren werden, wenn diese Einschränkung in Kraft ist, unter anderem bei Webbrowsern, `WebKitGTK`, `Flatpak` und der Erstellung von Vorschaubildern in `GNOME`.

Das Debian-spezifische sysctl `kernel.unprivileged_userns_clone=0` hat einen ähnlichen Effekt, ist aber überholt.

5.1.14 Linux deaktiviert standardmäßig unpriviligierte Aufrufe von bpf()

Ab `Linux` 5.10 unterbindet Debian standardmäßig unpriviligierte Aufrufe von bpf(). Allerdings kann ein Admin dies - falls erforderlich - später anpassen, indem der Sysctl `kernel.unprivileged_bpf_disabled` auf 0 oder 1 gesetzt wird.

Falls Sie unpriviligierte Aufrufe von bpf() weiter erlauben möchten, setzen Sie diesen Sysctl:

```
kernel.unprivileged_bpf_disabled = 0
```

Hintergrundinformationen zur dieser Änderung der Standardeinstellung finden Sie im Fehlerbericht #990411 (`https://bugs.debian.org/990411`), in dem diese Änderung angefordert wurde.

5.1.15 redmine fehlt in Bullseye

Das Paket `redmine` wird in Bullseye nicht angeboten, da es zu spät war, um von der alten `rails`-Version (die das Ende der Unterstützung durch die Upstream-Autoren erreicht hat und nur noch begrenzt Korrekturen für Sicherheitsprobleme erhält) auf die neue, in Bullseye enthaltene Version zu migrieren. Die Betreuer von `Ruby Extras` sind dicht an den Upstream-Autoren dran und werden eine neue Version über backports (`https://backports.debian.org/`) veröffentlichen, sobald sie freigegeben ist und die Pakete funktionieren. Falls Sie mit einem Upgrade darauf nicht warten möchten, können Sie eine VM (virtuelle Maschine) oder einen Container nutzen, in dem Buster läuft, um diese spezielle Anwendung zu isolieren.

5.1.16 Exim 4.94

Bitte sehen Sie die Bullseye-Version von Exim als *großes* Exim-Upgrade an. Sie führt ein Konzept ein, das von nicht-vertrauenswürden Quellen empfangene Daten als unrein ansieht, wie z.B. Nachrichtenabsender oder Empfänger. Solche unreinen Daten (z.B. `$local_part` oder `$domain`) können nicht als Teil von Datei- oder Verzeichnisname oder Befehlsnamen genutzt werden.

Dies wird Konfigurationen *unbrauchbar machen*, die nicht entsprechend angepasst werden. Alte Exim-Konfigurationsdateien werden unverändert auch nicht mehr funktionieren; die neue Konfiguration muss installiert und lokale Änderungen dann erneut eingepflegt werden.

Typische Beispiele, die nicht mehr funktionieren werden:

- Auslieferung an `/var/mail/$local_part`. Verwenden Sie stattdessen `$local_part_data` in Kombination mit `check_local_user`.
- die Verwendung von

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

  statt

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

  für die Alias-Datei einer virtuellen Domain.

Die zugrunde liegende Strategie, mit dieser Änderung umzugehen ist, das Ergebnis einer zusätzlicher Abfrage zu verwenden, statt dem (von extern empfangenen) Originalwert.

Um das Upgrade zu erleichtern, gibt es eine neue Haupt-Konfigurationsoption, die solche Unreine-Daten-Fehler auf Warnungen herabstuft, und die es somit ermöglicht, die alte Konfiguration mit der neuen Exim-Version laufen zu lassen. Um diese Funktion zu nutzen, fügen Sie

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

zu Ihrer Exim-Konfiguration (z.B. zu `/etc/exim4/exim4.conf.localmacros`) hinzu, *bevor* Sie das Upgrade starten, und schauen Sie in der Logdatei nach solchen Warnungen. Dies ist nur ein vorübergehender Workaround, der bereits wieder zur Löschung vorgesehen ist.

5.1.17 SCSI-Geräteerkennung nicht mehr sicher vorhersagbar

Aufgrund von Änderungen im Linux-Kernel ist das Ergebnis der Erkennung von SCSI-Geräten nicht mehr deterministisch (sicher vorhersagbar). Dies könnte ein Problem sein für Installationen, die sich auf die Reihenfolge der erkannten Geräte verlassen. Zwei mögliche Alternativen sind die Verwendung von Links in `/dev/disk/by-path` oder einer `udev`-Regel, wie in diesem Mailinglisten-Beitrag (`https://lore.kernel.org/lkml/59eedd28-25d4-7899-7c3c-89fe7fdd4b43@acm.org/`) empfohlen.

5.1.18 rdiff-backup erfordert lockstep-Upgrade auf Server und Client

Die Netzwerk-Protokolle der Versionen 1 und 2 von `rdiff-backup` sind inkompatibel. Das bedeutet, dass Sie lokal und fern die gleiche Version (entweder 1 oder 2) von `rdiff-backup` verwenden müssen. Da Buster die Version 1.2.8 enthält und Bullseye die Version 2.0.5, werden `rdiff-backup`-Läufe nicht mehr funktionieren, wenn Sie nur das lokale System oder nur das ferne System von Buster auf Bullseye hochrüsten.

Die Version 2.0.5 von `rdiff-backup` ist im buster-backports-Archiv verfügbar, siehe backports (`https://backports.debian.org/`). Dies gibt Ihnen die Möglichkeit, zuerst nur das `rdiff-backup`-Paket auf Ihren Buster-Systemen hochzurüsten, und dann unabhängig voneinander die Systeme auf Bullseye hochzuziehen.

5.1.19 Probleme mit Intel CPU Microcode

Das aktuell in bullseye und buster-security enthaltene `intel-microcode`-Paket (schauen Sie unter DSA-4934-1 (`https://www.debian.org/security/2021/dsa-4934`)) hat bekanntermaßen zwei gravierende Fehler. Für einige CoffeeLake-CPUs könnte dieses Update Netzwerkschnittstellen außer Funktion setzen (`https://github.com/intel/Intel-Linux-Processor-Microcode-Data-Files/issues/56`), die `firmware-iwlwifi` verwenden, und bei einigen Skylake-R0/D0-CPUs auf Systemen mit stark veralteter Firmware (BIOS) könnte das System beim Booten hängen bleiben (`https://github.com/intel/Intel-Linux-Processor-Microcode-Data-Files/issues/31`).

Wenn Sie das Update von DSA-4934-1 wegen eines dieser Probleme zurückgehalten haben, oder das Security-Archiv nicht aktiviert haben, seien Sie gewarnt, dass beim Upgrade des `intel-microcode`-Pakets auf die Bullseye-Version Ihr System beim Booten hängen könnte oder iwlwifi-Schnittstellen nicht mehr funktionieren könnten. In diesem Fall können Sie das System wiederherstellen, indem Sie das Laden von Microcode beim Booten deaktivieren; schauen Sie in die Anweisungen in der DSA (oder in die `README.Debian`-Datei im `intel-microcode`-Paket).

5.1.20 Upgrades, die libgc1c2 beinhalten, benötigen zwei Durchläufe

Pakete, die in Buster von `libgc1c2` abhängen (z.B. `guile-2.2-libs`), könnten beim ersten vollständigen Upgrade-Durchlauf auf Bullseye zurückgehalten werden. Das Upgrade ein weiteres Mal zu starten, sollte das Problem beheben. Hintergrundinfos zu diesem Problem finden Sie im Fehlerbericht #988963 (`https://bugs.debian.org/988963`).

5.1.21 fail2ban kann mittels mail aus bsd-mailx keine E-Mails versenden

Das `fail2ban`-Paket kann konfiguriert werden, E-Mail-Benachrichtigungen zu versenden. Es verwendet dazu **mail**, das von verschiedenen Paketen in Debian bereitgestellt wird. Eine Sicherheitsaktualisierung direkt vor der Veröffentlichung von Bullseye (erforderlich auf Systemen, die **mail** aus dem Paket `mailutils` nutzen) hat diese Funktionalität für Systeme beschädigt, die **mail** aus dem `bsd-mailx`-Paket verwenden. Nutzer von `fail2ban` in Kombination mit `bsd-mailx`, die möchten, dass `fail2ban`

E-Mails versendet, sollten entweder auf ein anderes Paket wechseln, das **mail** bereitstellt, oder den Upstream commit (`https://github.com/fail2ban/fail2ban/commit/410a6ce5c80dd981c22752da034f2529`) rückgängig machen, der die Zeichenfolge "`-E 'set escape'`" an mehreren Stellen in `/etc/fail2ban/action.d/` hinzugefügt hat.

5.1.22 Keine neuen SSH-Verbindungen möglich während des Upgrades

Obwohl bereits vorhandene Secure-Shell- (SSH) Verbindungen während des Upgrades wie gewohnt weiter funktionieren sollten, ist aufgrund unglücklicher Umstände die Zeitspanne, während derer keine neuen SSH-Verbindungen aufgebaut werden können, länger wie sonst. Falls das Upgrade über eine SSH-Verbindung ausgeführt wird, die währenddessen unter Umständen unterbrochen werden könnte, wird empfohlen, das Paket `openssh-server` separat zu aktualisieren, bevor das vollständige System-Upgrade gestartet wird.

5.1.23 Open vSwitch upgrade requires interfaces(5) change

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

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

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

5.1.24 Dinge, die vor dem Neustart erledigt werden sollten

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

5.2 Dinge, die nicht auf den Upgrade-Prozess beschränkt sind

5.2.1 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.

5.2.1.1 Sicherheitsstatus von Webbrowsern und deren Rendering-Engines

Debian 11 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-(Orignal-)Versionen hochzurüsten. Browser, die auf Engines wie „webkit", „qtwebkit" und „khtml"[1] aufbauen, sind daher in Bullseye zwar enthalten, es besteht jedoch für sie keine Sicherheitsunterstützung. Diese Browser sollten nicht für Verbindungen zu Websites verwendet werden, denen

[1] 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 und dem neuen wpewebkit.

Sie nicht vertrauen. Die webkit2gtk- und wpewebkit-Engines sind 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.

5.2.1.2 OpenJDK 17

Debian Bullseye enthält eine Vorabversion von `OpenJDK 17` (die nächste zu erwartende `LTS`-Version nach `OpenJDK 11`), um den ziemlich lästigen Bootstrap-Prozess zu vermeiden. Der Plan für Debian Bullseye ist, für `OpenJDK 17` eine Aktualisierung auf die finale Upstream-Version zu bekommen, die für Oktober 2021 angekündigt ist. Anschließend beabsichtigen wir, soweit möglich Sicherheitsaktualisierungen hierfür bereitzustellen, aber Benutzer sollten keine regelmäßigen quartalsmäßigen Updates erwarten.

5.2.1.3 Go-basierte Pakete

Debian's Infrastruktur hat derzeit Probleme beim Neubau von Paketentypen, die systematischen Gebrauch von statischer Verlinkung machen. Vor Buster war dies in der Praxis noch kein Thema, aber das Anwachsen des Go-Ecosystems bedeutet, dass Go-basierte Pakete jetzt nur noch eingeschränkt von Debians Sicherheitsunterstützung abgedeckt sein werden, bis die Infrastruktur dahingehend entsprechend verbessert wurde.

Falls Aktualisierungen für Go-Development-Bibliotheken zugesichert werden, können diese nur im Rahmen von Zwischenveröffentlichungen ausgeliefert werden, was solche Updates zeitlich verzögern können.

5.2.2 Zugriff auf die GNOME-Einstellungen ohne Maus

Ohne Zeigegerät/Maus gibt es keinen direkten Weg, um Einstellungen im GNOME-Einstellungen-Programm (aus dem `gnome-control-center`-Paket) durchzuführen. Um dieses Problem zu umgehen, können Sie von der Seitenleiste (links) zum Hauptfenster navigieren, indem Sie zweimal die Taste **Pfeil rechts** drücken. Um zurück zur Seitenleiste zu gelangen, öffnen Sie eine Suche mittels Strg + F, tippen irgendetwas ein, und drücken dann **Esc**, um die Suche abzubrechen. Jetzt können Sie die Tasten **Pfeil hoch** und **Pfeil runter** benutzen, um in der Seitenleiste zu navigieren. Es ist leider nicht möglich, Suchergebnisse über die Tastatur auszuwählen.

5.2.3 Die `rescue`-Boot-Option ist nicht ohne root-Passwort nutzbar

Mit der Implementation von `sulogin`, die seit Buster genutzt wird, erfordert das Booten mit der `rescue`-Option immer ein root-Passwort. Falls keins festgelegt wurde, führt dies dazu, dass der Rescue-Modus letztlich nicht nutzbar ist. Allerdings ist es trotzdem möglich, mit dem Kernel-Parameter `init=/sbin/sulogi` `--force` zu booten.

Um etwas vergleichbares zu erreichen, wann immer systemd im Rescue-Modus bootet, (auch bekannt als Single-Mode; siehe systemd(1) (`https://manpages.debian.org//bullseye/systemd/systemd.1.html`)), führen Sie **sudo systemctl edit rescue.service** aus und erstellen eine Datei, die folgendes enthält:

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

Es könnte aber auch (oder stattdessen) nützlich sein, dies für die `emergency.service`-Unit durchzuführen, die im Falle bestimmter Fehler (siehe systemd.special(7) (`https://manpages.debian.org//bullseye/systemd/systemd.special.7.html`)) *automatisch* gestartet wird, oder falls `emergency` zur Kernel-Befehlszeile hinzugefügt wird (also z.B. in Fällen, wenn das System nicht über den Rescue-Modus wiederbelebt werden kann).

Hintergrundinformationen und eine Diskussion über diesbezügliche Sicherheitsaspekte finden Sie unter #802211 (`https://bugs.debian.org//802211`).

5.3 Überalterungen und Missbilligungen

5.3.1 Nennenswerte veraltete Pakete

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

- Das `lilo`-Paket wurde aus Bullseye entfernt. Sein Nachfolger als Bootloader ist `grub2`.
- Die Version 3 des Mailinglisten-Managers Mailman ist die einzige verfügbare in dieser Veröffentlichung. 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 Mailman-Version 2.1 ist nicht mehr verfügbar (dies war das Paket `mailman`). Diese Version hat eine Abhängigkeit von Python 2, welches nicht mehr in Debian enthalten ist.

  Für Instruktionen zur Aktualisierung lesen Sie Mailman's Migrationsdokumentation (`https://docs.mailman3.org/en/latest/migration.html`).
- Der Linux-Kernel bietet keine Unterstützung mehr für `isdn4linux` (i4l). Daher wurden auch die Userland-Pakete `isdnutils`, `isdnactivecards`, `drdsl` und `ibod` aus den Archiven entfernt.
- Die veralteten libappindicator-Bibliotheken werden nicht länger angeboten. Als Ergebnis sind die zugehörigen Pakete `libappindicator1`, `libappindicator3-1` und `libappindicator-dev` ebenfalls nicht mehr verfügbar. Dies wird vermutlich zu Paketabhängigkeits-Problemen bei Fremdsoftware führen, die noch von libappindicator abhängen, um Benachrichtigungen oder Systemanzeigen (system tray) zu unterstützen.

  Debian verwendet `libayatana-appindicator` als Nachfolger für libappindicator. Für weitere technische Hintergrundinformationen lesen Sie diese Ankündigung (`https://lists.debian.org/debian-devel/2018/03/msg00506.html`).
- Debian bietet das Paket `chef` nicht mehr an. Wenn Sie chef für Ihr Konfigurations-Management verwenden, ist die beste Variante für ein Upgrade vermutlich die, auf Pakete von Chef Inc (`https://www.chef.io/`) hochzurüsten.

  Hintergrundinformationen zur Entfernung finden Sie im Removal request (`https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=963750`).
- Python 2 hat das Ende seiner Lebenszeit bereits überschritten, und wird keine Sicherheitsaktualisierungen mehr erhalten. Es wird nicht mehr unterstützt, um Anwendungen laufen zu lassen und Pakete, die darauf aufbauen, sind entweder auf Python 3 konvertiert oder entfernt worden. Allerdings enthält Debian Bullseye noch die Version Python 2.7, sowie eine kleinere Anzahl von Bauwerkzeugen für Python 2, wie z.B. `python-setuptools`. Diese sind jedoch nur vorhanden, da sie noch benötigt werden, um einige wenige Anwendungen zu bauen, die noch nicht auf Python 3 konvertiert wurden.
- Das `aufs-dkms`-Paket ist nicht Teil von Bullseye. Die meisten `aufs-dkms`-Nutzer sollten nach `overlayfs` wechseln können, das eine ähnliche Funktionalität mit Kernel-Unterstützung bietet. Allerdings kann es Debian-Installationen geben, die auf einem Dateisystem liegen, welches nicht mit `overlayfs` kompatibel ist, z.B. `xfs` ohne `d_type`. Nutzer von `aufs-dkms` werden daher aufgefordert, vor dem Upgrade auf Bullseye von `aufs-dkms` zu einer Alternative zu migrieren.
- The network connection manager `wicd` will no longer be available after the upgrade, so to avoid the danger of losing connectivity users are recommended to switch before the upgrade to an alternative such as `network-manager` or `connman`.

5.3.2 Missbilligte Komponenten für Bullseye

Mit der nächsten Veröffentlichung von Debian 12 (Codename Bookworm) werden einige Funktionalitäten missbilligt sein. Nutzer müssen auf andere Alternativen umsteigen, um Schwierigkeiten nach dem Upgrade auf Debian 12 zu vermeiden.
Dazu gehören folgende Funktionalitäten:

- Die alten Rechtfertigungen für das Dateisystem-Layout mit den Verzeichnissen `/bin`, `/sbin` und `/lib` getrennt von ihren Äquivalenten in `/usr` gelten heutzutage nicht mehr; lesen Sie dazu Freedesktop.org summary (`https://www.freedesktop.org/wiki/Software/systemd/TheCaseForTheUs`) Debian Bullseye wird die letzte Debian-Veröffentlichung sein, die das alte Layout unterstützt, in dem oben erwähnte Verzeichnisse nicht unter /usr zusammengeführt sind (non-merged-usr layout). Für Systeme, die dieses alte Layout verwenden, und die ohne Neuinstallation auf Bullseye hochgerüstet werden, gibt es das `usrmerge`-Paket, das - falls gewünscht - die Umstellung durchgeführt.

- Bullseye ist die letzte Debian-Version, die **apt-key** enthält. Die Schlüsselverwaltung sollte stattdessen über Dateien erfolgen, die in `/etc/apt/trusted.gpg.d` abgelegt werden (in binärer Form, wie sie von **gpg --export** mit einer `.gpg`-Dateierweiterung erzeugt werden, oder in verschlüsseltem ASCII mit `.asc`-Erweiterung.

  Ein Ersatz für **apt-key list**, um den Schlüsselring händisch untersuchen zu können, ist in Planung, aber die Arbeit dafür hat noch nicht begonnen.

- Die `slapd` Datenbank-Backends slapd-bdb(5) (`https://manpages.debian.org//bullseye/slapd/slapd-bdb.5.html`), slapd-hdb(5) (`https://manpages.debian.org//bullseye/slapd/slapd-hdb.5.html`) und slapd-shell(5) (`https://manpages.debian.org//bullseye/slapd/slapd-shell.5.html`) sind zurückgezogen worden und werden nicht in Debian 12 enthalten sein. LDAP-Datenbanken, die das `bdb`- oder das `hdb`-Backend verwenden, sollten nach slapd-mdb(5) (`https://manpages.debian.org//bullseye/slapd/slapd-mdb.5.html`) migriert werden.

  Desweiteren sind die slapd-perl(5) (`https://manpages.debian.org//bullseye/slapd/slapd-perl.5.html`)- und slapd-sql(5) (`https://manpages.debian.org//bullseye/slapd/slapd-sql.5.html`)-Backends veraltet und könnten in zukünftigen Veröffentlichungen entfernt werden.

  Das OpenLDAP-Projekt unterstützt keine zurückgezogenen oder veralteten Backends. Die Unterstützung für diese Backends in Debian 11 erfolgt lediglich auf Best-Effort-Basis (wir tun, was wir können).

5.3.3 Nicht mehr unterstützte Hardware

Für eine Reihe von armel-basierten Geräten, die in Buster unterstützt wurden, ist es aufgrund von Hardware-Einschränkungen nicht mehr praktikabel, den erforderlichen `Linux`-Kernel zu bauen. Die aufgrunddessen nicht mehr unterstützten Geräte sind:

- QNAP Turbo Station (TS-xxx)
- HP Media Vault mv2120

Nutzer dieser Plattformen, die trotzdem auf Bullseye hochrüsten möchten, sollten die APT-Quellen für Buster aktiviert lassen. Vor dem Upgrade sollten sie deshalb eine APT-preferences-Datei mit folgendem Inhalt erstellen:

```
Package: linux-image-marvell
Pin: release n=buster
Pin-Priority: 900
```

Die Sicherheitsunterstützung für diese Konstellation ist nur bis zum Lebensende von Buster gewährleistet.

5.4 Bekannte gravierende Fehler

Obwohl Debian-Veröffentlichungen nur freigegeben werden, wenn sie fertig sind, heißt dies unglücklicherweise nicht, dass keine bekannten Fehler existieren. Als Teil des Release-Prozesses werden alle Fehler mit Schweregrad serious oder höher aktiv vom Release-Team verfolgt, daher gibt es in Debians Fehlerdatenbank (`https://bugs.debian.org/`) einen Überblick all der Fehler (`https://bugs.debian.org/cgi-bin/pkgreport.cgi?users=release.debian.org@packages.debian.org;`

tag=bullseye-can-defer), die im letzten Schritt der Freigabe von bullseye als "zu ignorieren" gekennzeichnet wurden. Folgende Fehler betreffen bullseye zum Zeitpunkt der Veröffentlichung und sollten hier erwähnt werden:

Fehlernummer	Quell- oder Binärpaket	Beschreibung
922981 (https://bugs.debian.org/922981)	ca-certificates-java	ca-certificates-java: /etc/ca-certificates/update.d/jks-keystore doesn't update /etc/ssl/certs/java/cacerts
990026 (https://bugs.debian.org/990026)	cron	cron: Reduced charset in MAILTO causes breakage
991081 (https://bugs.debian.org/991081)	gir1.2-diodon-1.0	gir1.2-diodon-1.0 lacks dependencies
990318 (https://bugs.debian.org/990318)	python-pkg-resources	python-pkg-resources: please add Breaks against the unversioned python packages
991449 (https://bugs.debian.org/991449)	fail2ban	fix for CVE-2021-32749 breaks systems with mail from bsd-mailx
990708 (https://bugs.debian.org/990708)	mariadb-server-10.5,galera	mariadb-server-10.5: upgrade problems due to galera-3 -> galera-4 switch
980429 (https://bugs.debian.org/980429)	src:gcc-10	g++-10: spurious c++17 mode segmentation fault in append_to_statement_list_1 (tree-iterator.c:65)
980609 (https://bugs.debian.org/980609)	src:gcc-10	missing i386-cpuinfo.h
984574 (https://bugs.debian.org/984574)	gcc-10-base	gcc-10-base: please add Breaks: gcc-8-base (<< 8.4)
984931 (https://bugs.debian.org/984931)	git-el	git-el,elpa-magit: fails to install: /usr/lib/emacsen-common/packages/install/git emacs failed at /usr/lib/emacsen-common/lib.pl line 19, <TSORT> line 7.
987264 (https://bugs.debian.org/987264)	git-el	git-el: fails to install with xemacs21
991082 (https://bugs.debian.org/991082)	gir1.2-gtd-1.0	gir1.2-gtd-1.0 has empty Depends
948739 (https://bugs.debian.org/948739)	gparted	gparted should not mask .mount units
984714 (https://bugs.debian.org/984714)	gparted	gparted should suggest exfat-progs and backport the commit that rejects exfat-utils
968368 (https://bugs.debian.org/968368)	ifenslave	ifenslave: Option bond-master fails to add interface to bond
990428 (https://bugs.debian.org/990428)	ifenslave	ifenslave: Bonding not working on bullseye (using bond-slaves config)
991113 (https://bugs.debian.org/991113)	libpam-chroot	libpam-chroot installs pam_chroot.so into the wrong directory
989545 (https://bugs.debian.org/989545)	src:llvm-toolchain-11	libgl1-mesa-dri: si_texture.c:1727 si_texture_transfer_map - failed to create temporary texture to hold untiled copy

Fehlernummer	Quell- oder Binärpaket	Beschreibung
982459 (https://bugs.debian.org/982459)	mdadm	mdadm --examine in chroot without /proc,/dev,/sys mounted corrupts host's filesystem
981054 (https://bugs.debian.org/981054)	openipmi	openipmi: Missing dependency on kmod
948318 (https://bugs.debian.org/948318)	openssh-server	openssh-server: Unable to restart sshd restart after upgrade to version 8.1p1-2
991151 (https://bugs.debian.org/991151)	procps	procps: dropped the reload option from the init script, breaking corekeeper
989103 (https://bugs.debian.org/989103)	pulseaudio	pulseaudio regressed on control = Wave configuration
984580 (https://bugs.debian.org/984580)	libpython3.9-dev	libpython3.9-dev: missing dependency on zlib1g-dev
990417 (https://bugs.debian.org/990417)	src:qemu	openjdk-11-jre-headless: running java in qemu s390 gives a SIGILL at C [linux-vdso64.so.1 + 0x6f8] _kernel_getcpu + 0x8
859926 (https://bugs.debian.org/859926)	speech-dispatcher	breaks with pulse-audio as output when spawned by speechd-up from init system
932501 (https://bugs.debian.org/932501)	src:squid-deb-proxy	squid-deb-proxy: daemon does not start due to the conf file not being allowed by apparmor
991588 (https://bugs.debian.org/991588)	tpm2-abrmd	tpm2-abrmd should not use Requires = systemd-udev-settle.service in its unit
991939 (https://bugs.debian.org/991939)	libjs-bootstrap4	libjs-bootstrap4: broken symlinks: /usr/share/javascript/bootstrap4/css/bootstrap*.css.map -> ../../../nodejs/bootstrap/dist/css/bootstrap*.c
991822 (https://bugs.debian.org/991822)	src:wine	src:wine: dh_auto_clean deletes unrelated files outside of package source
988477 (https://bugs.debian.org/988477)	src:xen	xen-hypervisor-4.14-amd64: xen dmesg shows (XEN) AMD-Vi: IO_PAGE_FAULT on sata pci device
991788 (https://bugs.debian.org/991788)	xfce4-settings	xfce4-settings: black screen after suspend when laptop lid is closed and re-opened

Kapitel 6

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/`) und im Debian Wiki (`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/`) 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`).

Für weitere Informationen zum OFTC besuchen Sie bitte dessen Website (`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 bedürfenden 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 Buster-Systems vor dem Upgrade

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

A.1 Upgrade Ihres Buster-Systems

Dem Grunde nach ist dies nichts anderes als jedes bisherige Upgrade von Buster. Der einzige Unterschied besteht darin, dass Sie zuerst sicherstellen müssen, dass Ihre Paketliste noch Referenzen für buster 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 Buster.

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//bullseye/apt/sources.list.5.html`)) auf „stable“ beziehen, zeigen sie effektiv schon auf Bullseye-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 Bullseye installiert haben, ergibt es wahrscheinlich keinen Sinn mehr, Pakete aus Buster 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 `buster`.

Falls Zeilen vorkommen, die mit `deb file:` oder `URIs: file:` beginnen, müssen Sie selbst überprüfen, ob der darin angegebene Ort ein Archiv von Buster oder Bullseye 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 Bullseye aktualisieren, wird empfohlen, alte Konfigurationsdateien (wie `*.dpkg-{new,old}`-Dateien in `/etc`) vom System zu entfernen.

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