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

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

19. Oktober 2022
Hinweise zur Debian-Veröffentlichung Version 11 (Bullseye) auf ARM EABI

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

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

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

# Inhaltsverzeichnis

1 Einführung
   1.1 Fehler in diesem Dokument berichten .............................................. 1
   1.2 Upgrade-Berichte zur Verfügung stellen ........................................... 1
   1.3 Quelltext dieses Dokuments ............................................................. 2

2 Was ist neu in Debian 11
   2.1 Unterstützte Architekturen ............................................................... 3
   2.2 Was ist neu in der Distribution? ....................................................... 3
      2.2.1 Desktop-Umgebungen und bekannte Pakete ...................................... 3
      2.2.2 Treiberloses Scannen und Drucken ............................................... 4
         2.2.2.1 CUPS und treiberloses Drucken ............................................. 4
         2.2.2.2 SANE und treiberloses Scannen ............................................ 5
      2.2.3 Neuer generischer open-Befehl .................................................... 5
      2.2.4 Control groups v2 ...................................................................... 5
      2.2.5 Dauerhaftes systemd-Journal ...................................................... 5
      2.2.6 Neue Fcitx-5-Eingabemethode ..................................................... 5
      2.2.7 Neuigkeiten vom Debian Med Blend ............................................. 5
      2.2.8 Kernel-Unterstützung für exFAT .................................................. 6
      2.2.9 Verbesserte Übersetzungen von Handbuchseiten ............................... 6
      2.2.10 Verbesserte Unterstützung für alternative Init-Systeme ...................... 6

3 Installationssystem .......................................................... 7
   3.1 Was ist neu im Installationssystem? .................................................. 7
      3.1.1 Hilfe bei der Installation von Firmware ......................................... 7
      3.1.2 Automatisierte Installation ......................................................... 7
   3.2 Images für Container und virtuelle Maschinen .................................... 8

4 Upgrade von Debian 10 (Buster) ........................................... 9
   4.1 Vorbereiten des Upgrades .................................................................. 9
      4.1.1 Sichern aller Daten und Konfigurationsinformationen ...................... 9
      4.1.2 Die Benutzer vorab informieren .................................................... 9
      4.1.3 Vorbereitung auf die Deaktivierung von Diensten ............................. 10
      4.1.4 Vorbereitungen für eine Systemwiederherstellung ......................... 10
         4.1.4.1 Shell zur Fehleranalyse während des Bootens mit Initrd ............... 10
         4.1.4.2 Shell zur Fehleranalyse während des Bootens mit systemd ............. 11
      4.1.5 Vorbereiten einer sicheren Umgebung für das Upgrade .................... 11
   4.2 Start des Upgrades von einem „reinen“ Debian-System ......................... 11
      4.2.1 Upgrade auf Debian 10 (Buster) .................................................. 12
      4.2.2 Pakete entfernen, die nicht von Debian stammen ............................... 12
      4.2.3 Upgrade auf die letzte Zwischenveröffentlichung ............................... 12
      4.2.4 Vorbereiten der Paketdatenbank .................................................. 12
      4.2.5 Veraltete Pakete entfernen .......................................................... 12
      4.2.6 Bereinigen alter Konfigurationsdateien ........................................ 12
      4.2.7 Der Bereich für Sicherheitsaktualisierungen (Security) ...................... 12
      4.2.8 Der Bereich für vorgeschlagene Aktualisierungen („proposed-updates“) .. 13
      4.2.9 Inoffizielle Quellen .................................................................... 13
      4.2.10 APT Pinning deaktivieren ............................................................ 13
      4.2.11 Paketstatus überprüfen ............................................................... 13
   4.3 Die APT source-list-Dateien vorbereiten ............................................ 14
      4.3.1 APT-Internet-Quellen hinzufügen .................................................. 14
      4.3.2 APT-Quellen für einen lokalen Spiegel hinzufügen ............................ 15
      4.3.3 APT-Quellen für optische Medien hinzufügen .................................. 15
   4.4 Upgrades von Paketen durchführen .................................................... 15
      4.4.1 Aufzeichnung der Sitzung .............................................................. 16
## INHALTSVERZEICHNIS

4.4.2 Aktualisieren der Paketliste ........................................... 16
4.4.3 Sicherstellen, dass genügend Speicherplatz für das Upgrade zur Verfügung steht 17
4.4.4 Minimales System-Upgrade ............................................. 19
4.4.5 Upgrade des Systems .................................................... 19
4.5 Mögliche Probleme während des Upgrades ............................ 20
4.5.1 dist-upgrade schlägt fehl mit „Could not perform immediate configuration“ 20
4.5.2 Zu erwartende Paketentfernungen ................................. 20
4.5.3 Konflikte oder Pre-Depends-Schleifen ............................ 20
4.5.4 Dateikonflikte .......................................................... 20
4.5.5 Konfigurationsänderungen .................. .......................... 21
4.5.6 Ändern der aktuellen Sitzung auf die Konsole ................. 21
4.6 Upgrade des Kernels und zugehöriger Pakete ....................... 21
4.6.1 Ein Kernel-Metapaket installieren ................................. 21
4.7 Vorbereiten auf die nächste Veröffentlichung ...................... 22
4.7.1 Vollständiges Löschen entfernter Pakete ......................... 22
4.8 Veraltete Pakete .......................................................... 23
4.8.1 Übergangs-Dummy-Pakete ........................................... 23

5 Dinge, die Sie über Bullseye wissen sollten ........................................ 25
5.1 Upgrade-spezifische Themen für Bullseye ......................... 25
5.1.1 Das XFS-Dateisystem unterstützt nicht mehr die Optionen barrier/nobarrier 25
5.1.2 Geändertes Layout im Security-Archiv .......................... 25
5.1.3 Passwort-Hash verwendet standardmäßig yescrypt ............ 25
5.1.4 NSS-, NIS- und NIS+-Unterstützung benötigt neue Pakete .... 26
5.1.5 Behandlung von Konfigurationsdatei-Fragmenten in unbound 26
5.1.6 Missbilligung einiger rsync-Parameter ........................ 26
5.1.7 Behandlung von Addons in vim .................................. 26
5.1.8 OpenStack und cgroups v1 ......................................... 26
5.1.9 OpenStack API: Regel-Dateien .................................. 27
5.1.10 sendmail nicht verfügbar während des Upgrades .......... 27
5.1.11 FUSE 3 ............................................................... 27
5.1.12 GnuPG options-Datei .............................................. 27
5.1.13 Linux aktiviert standardmäßig User Namespaces ............ 27
5.1.14 Linux deaktiviert standardmäßig unprivilegierte Aufrufe von bpf() 28
5.1.15 redmine fehlt in Bullseye .......................................... 28
5.1.16 Exim 4.94 ............................................................. 28
5.1.17 SCSI-Geräteerkennung nicht mehr sicher vorhersehbar .... 29
5.1.18 rdiff-backup erfordert lockstep-Upgrade auf Server und Client 29
5.1.19 Probleme mit Intel CPU Microcode ............................. 29
5.1.20 Upgrades, die libgc1c2 beinhalten, benötigen zwei Durchläufe 29
5.1.21 fail2ban kann mittels mail aus bsd-mailx keine E-Mails versenden 29
5.1.22 Keine neuen SSD-Verbindungen möglich während des Upgrades 29
5.1.23 Open vSwitch upgrade requires interfaces(5) change .... 30
5.1.24 Dinge, die vor dem Neustart erledigt werden sollten ....... 30
5.2 Dinge, die nicht auf den Upgrade-Prozess beschränkt sind ........ 30
5.2.1 Einschränkungen bei der Sicherheitsunterstützung ............. 30
5.2.1.1 Sicherheitsstatus von Webbrowsern und deren Rendering-Engines 30
5.2.1.2 OpenJDK 17 ..................................................... 30
5.2.1.3 Go-basierte Pakete ............................................ 31
5.2.2 Zugriff auf die GNOME-Einstellungen ohne Maus ............ 31
5.2.3 Die rescue-Boot-Option ist nicht ohne root-Passwort nutzbar 31
5.3 Überalterungen und Missbilligungen ................................. 31
5.3.1 Nennenswerte veraltete Pakete .................................. 31
5.3.2 Missbilligte Komponenten für Bullseye ......................... 32
5.3.3 Nicht mehr unterstützte Hardware ................................. 33
5.4 Bekannte gravierende Fehler .......................................... 33
6 Zusätzliche Informationen zu Debian
   6.1 Weitere Lektüre ........................................ 37
   6.2 Hilfe bekommen ........................................ 37
      6.2.1 Mailinglisten ...................................... 37
      6.2.2 Internet Relay Chat ................................ 37
   6.3 Fehler berichten ....................................... 37
   6.4 Zu Debian beitragen .................................... 38

7 Glossar ...................................................... 39

A Verwalten Ihres Buster-Systems vor dem Upgrade ............... 41
   A.1 Upgrade Ihres Buster-Systems .............................. 41
   A.2 Überprüfen Ihrer Paketquellen (APT source-list-Dateien) .... 41
   A.3 Veraltete Konfigurationsdateien entfernen ................ 42

B Mitwirkende bei den Veröffentlichungshinweisen .................. 43

Index .................................................................. 45
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.


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:


- 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

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?


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:

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

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 Gerätmodell spezifischen Treibern.

2.2.2.1 CUPS und treiberloses Drucken


2.2.2.2 SANE und treiberloses Scannen


*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 das Seiten eines treiberlosen Backends eingerichtet wird, sobald es per USB angeschlossen ist.

2.2.3 Neuer generischer open-Befehl


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


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


2.2.7 Neukigkeit von 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.


### 2.2.8 Kernel-Unterstützung für exFAT


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


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.


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

3.2 Images für Container und virtuelle Maschinen


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.


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 Bedieneringabe während des Prozesses erfordert.

Wenn das zu aktualisierende System kritische Dienste für Ihre Nutzer oder für das Netzwerk bereitstellt, 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


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 Netzwerkebene 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.


4.1.4.1 Shell zur Fehleranalyse während des Bootens mit Initrd

Das initramfs-tools-Paket integriert eine Shell zur Fehleranalyse 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.

1Wenn 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.

2Zum 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.

3Diese Funktionalität kann deaktiviert werden, indem der Parameter panic=0 zu den Boot-Parametern hinzugefügt wird.
KAPITEL 4. UPGRADE VON DEBIAN 10 (BUSTER) 4.2. START DES UPGRADES VON EINEM


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 frühestmöglichen 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 /
```


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(in?installed, !in?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 Paketedatenbank

Bevor Sie das Upgrade starten, sollten Sie kontrollieren, ob noch ausstehende Aktionen in der Paketedatenbank 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.

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

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 '*.dkg-*' -o -name '*.ucf-*' -o -name '*.merge-error'
```

4.2.7 Der Bereich für Sicherheitsaktualisierungen (Security)

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


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:

```
# 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:

\[\text{Das Paketverwaltungssystem von Debian erlaubt es normalerweise nicht, dass ein Paket Dateien anderer Pakete entfernt oder ersetzt, es sei denn, es wurde definiert, dass es das andere Paket ersetzt.}\]
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.


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).

4.3.1 APT-Internet-Quellen hinzufügen


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/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):

```
```
KAPITEL 4. UPGRADE VON DEBIAN 10 (BUSTER)  4.4. UPGRADES VON PAKETEN DURCHFÜHREN

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

Statte 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.
**KAPITEL 4. UPGRADE VON DEBIAN 10 (BUSTER) 4.4. UPGRADES VON PAKETEN DURCHFÜHREN**

**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-bullseyeschnitt1.time -a ~/upgrade-bullseyeschnitt1. 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.


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

```
# scriptreplay ~/upgrade-bullseyeschnitt1.time ~/upgrade-bullseyeschnitt1.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
```
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.
```

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:

```bash
# 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 `I` und geben Sie `-i` ein, drücken Sie dann `S` und geben Sie `-installsize` ein. Nun wird Ihnen eine schöne Liste angezeigt, mit der Sie arbeiten können.


- 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:
   ```bash
   # apt clean
   ```

2. kopieren Sie das Verzeichnis `/var/cache/apt/archives` auf die USB-Festplatte:
   ```bash
   # cp -ax /var/cache/apt/archives /media/usbkey/
   ```

3. binden Sie das temporäre Cache-Verzeichnis in dem vorhandenen ein:
   ```bash
   # mount --bind /media/usbkey/archives /var/cache/apt/archives
   ```

4. stellen Sie nach dem Upgrade das ursprüngliche `/var/cache/apt/archives`-Verzeichnis wieder her:
   ```bash
   # 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.**
KAPITEL 4. UPGRADE VON DEBIAN 10 (BUSTER) 4.5. MÖGLICHE PROBLEME WÄHREND DES UPGRADES

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 'pakete'. 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


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`-Befehle 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>
```

20
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


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 verfügbare `linux-image`-Metapakete bekommen Sie mit:

```
# apt-cache search linux-image- | grep -i meta | grep -v transition
```
KAPITEL 4. UPGRADE VON DEBIAN 10 (BUSTER) 4.7. VORBEREITEN AUF DIE NÄCHSTE...

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
```


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


**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 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 einstellen5 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 werden 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'
```


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.


---

5So 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


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

5.1 Upgrade-spezifische Themen für Bullseye

Die Sicherheit gegen wörterbuchbasierte Angriffe zum Erraten von Passwörtern 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.


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

```plaintext
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


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


### 5.1.7 Behandlung von Addons in vim


### 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-Verzeichnisaum in `/sys/fs/cgroup` keine cgroupv1-Funktionen wie `/sys/fs/cgroup/blkio`, und aufgrund dessen wird `cgcreate -g blkio:foo` fehlschlagen. Für OpenStack-Nodes, auf denen `nova-compute` oder `cinder-volume` läuft, wird dringend empfohlen, die Parameter `systemd.unified_cgroup_hierarchy=false` und `systemd.legacy_systemd_cgroup_controller=false` zur Kernel-Befehlszeile hinzuzufügen, um die Standardeinstellungen zu überschreiben und die alte cgroup-Hierarchie weiter zu verwenden.
KAPITEL 5. DINGE, DIE SIE ÜBER BULLSEYE ...

5.1. UPGRADE-SPEZIFISCHE THEMEN FÜR ...

5.1.9 OpenStack API: Regel-Dateien


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.


5.1.10 sendmail nicht verfügbar während des Upgrades


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, zurückgelassen 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


5.1.13 Linux aktiviert standardmäßig User Namespaces


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_usersns_clone=0 hat einen ähnlichen Effekt, ist aber überholt.

27
**5.1.14 Linux deaktiviert standardmäßig unprivilegierter Aufrufe von bpf()**

Ab Linux 5.10 unterbindet Debian standardmäßig unprivilegierter 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 unprivilegierter 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**


**5.1.16 Exim 4.94**


Dies wird Konfigurationen unbrauchbar machen, die nicht entsprechend angepasst werden. Alte Exim-Konfigurationsdateien werden verändert 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.


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 Lösung vorgesehen ist.

28
5.1.17 **SCSI-Geräteerkennung nicht mehr sicher vorhersagbar**


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 hochrutschen.


5.1.19 **Probleme mit Intel CPU Microcode**


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`-Paktes 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 beschränkt, 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/410a6ce5c80dd981c22752da034a41c63966101) 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 Open vSwitch 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


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


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

---

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.
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 Debi ans 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


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


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.


- 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 Paketabhängigkeiten-Problemen bei Fremdsoftware führen, die noch von libappindicator abhängen, um Benachrichtigungen oder Systemanzeigen (system tray) zu unterstützen.


- 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).


- 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:


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 usmerge-Paket, das - falls gewünscht - die Umstellung durchgeführt.
KAPITEL 5. DINGE, DIE SIE ÜBER BULLSEYE …

5.4. BEKANnte GRAVIERenderE FEhler

• 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.


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 Debiants 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:

<table>
<thead>
<tr>
<th>Fehlernummer</th>
<th>Quell- oder Binärpaket</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>922981</td>
<td>ca-certificates-java</td>
<td>ca-certificates-java: /etc/ca-certificates-update.d/jks-keystore doesn't update /etc/ssl/certs/java/cacerts</td>
</tr>
<tr>
<td>990026</td>
<td>cron</td>
<td>cron: Reduced charset in MAILTO causes breakage</td>
</tr>
<tr>
<td>Fehlernummer</td>
<td>Quell- oder Binärpaket</td>
<td>Beschreibung</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>991081</td>
<td>girl.2-diodon-1.0</td>
<td>girl.2-diodon-1.0 lacks dependencies</td>
</tr>
<tr>
<td>990318</td>
<td>python-pkg-resources</td>
<td>python-pkg-resources: please add breaks against the unversioned python packages</td>
</tr>
<tr>
<td>991449</td>
<td>fail2ban</td>
<td>fix for CVE-2021-32749 breaks systems with mail from bsd-mailx</td>
</tr>
<tr>
<td>990708</td>
<td>mariadb-server-10.5,gale4</td>
<td>mariadb-server-10.5: upgrade problems due to galera-3 -&gt; galera-4 switch</td>
</tr>
<tr>
<td>980429</td>
<td>src:/gcc-10</td>
<td>g++ + -10: spurious c++17 mode segmentation fault in append_to_statement_list_1 (tree-iterator.c:65)</td>
</tr>
<tr>
<td>980609</td>
<td>src:/gcc-10</td>
<td>missing i386-cpuinfo.h</td>
</tr>
<tr>
<td>984574</td>
<td>gcc-10-base</td>
<td>gcc-10-base: please add Breaks: gcc-8-base (&lt; &lt; 8.4)</td>
</tr>
<tr>
<td>987264</td>
<td>git-el</td>
<td>git-el: fails to install with xemacs21</td>
</tr>
<tr>
<td>991082</td>
<td>girl.2-gtd-1.0</td>
<td>girl.2-gtd-1.0 has empty Depends</td>
</tr>
<tr>
<td>948739</td>
<td>gparted</td>
<td>gparted should not mask .mount units</td>
</tr>
<tr>
<td>984714</td>
<td>gparted</td>
<td>gparted should suggest exfat-progs and backport the commit that rejects exfat-utils</td>
</tr>
<tr>
<td>968368</td>
<td>ifenslave</td>
<td>ifenslave: Option bond-master fails to add interface to bond</td>
</tr>
<tr>
<td>990428</td>
<td>ifenslave</td>
<td>ifenslave: Bonding not working on bullseye (using bond-slaves config)</td>
</tr>
<tr>
<td>991113</td>
<td>libpam-chroot</td>
<td>libpam-chroot installs pam_chroot.so into the wrong directory</td>
</tr>
<tr>
<td>989545</td>
<td>src:llvm-toolchain-11</td>
<td>libgl1-mesa-dri: si_texture.c:1727 si_texture_transfer_map - failed to create temporary texture to hold untitled copy</td>
</tr>
<tr>
<td>982459</td>
<td>mdadm</td>
<td>mdadm --examine in chroot without /proc, /dev, /sys mounted corrupts host's filesystem</td>
</tr>
<tr>
<td>981054</td>
<td>openipmi</td>
<td>openipmi: Missing dependency on kmad</td>
</tr>
<tr>
<td>948318</td>
<td>openssh-server</td>
<td>openssh-server: Unable to restart sshd restart after upgrade to version 8.1p1-2</td>
</tr>
</tbody>
</table>
### Kapitel 5. Dinge, die Sie über Bullseye ...

#### 5.4. Bekannte gravierende Fehler

<table>
<thead>
<tr>
<th>Fehlernummer</th>
<th>Quell- oder Binärpaket</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>991151</td>
<td>procps</td>
<td>procps: dropped the reload option from the init script, breaking corekeeper</td>
</tr>
<tr>
<td>989103</td>
<td>pulseaudio</td>
<td>pulseaudio regressed on control=Wave configuration</td>
</tr>
<tr>
<td>984580</td>
<td>libpython3.9-dev</td>
<td>libpython3.9-dev: missing dependency on zlib1g-dev</td>
</tr>
<tr>
<td>990417</td>
<td>src:qemu</td>
<td>openjdk-11-jre-headless: running java in qemu s390 gives a SIGILL at C [linux-vdso64.so.1 + 0x6f8] __kernel_getcpu + 0x8</td>
</tr>
<tr>
<td>859926</td>
<td>speech-dispatcher</td>
<td>breaks with pulse-audio as output when spawned by speechd from init system</td>
</tr>
<tr>
<td>932501</td>
<td>src:squid-deb-proxy</td>
<td>squid-deb-proxy: daemon does not start due to the conf file not being allowed by apparmor</td>
</tr>
<tr>
<td>991588</td>
<td>tpm2-abrmd</td>
<td>tpm2-abrmd should not use Requires = systemd-udev-settle.service in its unit</td>
</tr>
<tr>
<td>991822</td>
<td>src:wine</td>
<td>src:wine: dh_auto_clean deletes unrelated files outside of package source</td>
</tr>
<tr>
<td>988477</td>
<td>src:xen</td>
<td>xen-hypervisor-4.14-amd64: xen dmesg shows (XEN) AMD-Vi: IO_PAGE_FAULT on sata pci device</td>
</tr>
<tr>
<td>991788</td>
<td>xfce4-settings</td>
<td>xfce4-settings: black screen after suspend when laptop lid is closed and re-opened</td>
</tr>
</tbody>
</table>
Kapitel 6

Zusätzliche Informationen zu Debian

6.1 Weitere Lektüre


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 bekomen

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


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).


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 Debiants

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 sind 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


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
KAPITEL 7. GLOSSAR

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


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.


WICHTIG

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:


Dieses Dokument wurde in viele Sprachen übersetzt. Vielen Dank an die Übersetzer!
Deutsche Übersetzung von: Holger Wansing.
Index

A
Apache, 4
B
BIND, 4
C
Calligra, 3
Cryptsetup, 4
D
DocBook XML, 2
Dovecot, 4
E
Exim, 4
G
GCC, 4
GIMP, 4
GNOME, 3
GNUcash, 4
GnuPG, 4
I
Inkscape, 4
K
KDE, 3
L
LibreOffice, 3
LXDE, 3
LXQt, 3
M
MariaDB, 4
MATE, 3
N
Nginx, 4
O
OpenJDK, 4
OpenSSH, 4
P
packages
apt, 2, 14, 15, 27
apt-listchanges, 19
aptitude, 12, 18, 22
aufs-dkms, 32
bsd-mailx, 29
cacertificates-java, 33
chef, 32
cinder-volume, 26
connman, 32
cron, 33
cups-browsed, 4
cups-daemon, 4
cups-filters, 4
dblatex, 2
debian-goodies, 18
debian-kernel-handbook, 22
debian-security-support, 30
doc-debian, 38
docbook-xsl, 2
dpkg, 2
drdsl, 32
dxfat-fuse, 6
dxfat-utils, 6
dxfatprogs, 6
fail2ban, 29, 34
firmware-iwlwifi, 29
fuse, 27
fuse3, 27
gcc-10-base, 34
gir1.2-diodon-1.0, 34
gir1.2-gtd-1.0, 34
git-el, 34
libre, 26
gnome-control-center, 31
gparted, 34
grub2, 31
guile-2.2-libs, 29
gvfs-fuse, 27
how-can-i-help, 38
ibod, 32
ifenslave, 34
initramfs-tools, 10, 21
intel-microcode, 29
ipp-usb, 4, 5
isdnactivecards, 32
isndnutils, 32
kio-fuse, 27
libappindicator-dev, 32
libappindicator1, 32
libappindicator3-1, 32
libayatana-appindicator, 32
libgc1c2, 29
libgs-bootstrap4, 35
libnss-nis, 26
libnss-nisplus, 26
libpam-chroot, 34
libpython3.9-dev, 35
libsane1, 5
lilo, 31
linux-image-*, 21
linux-image-amd64, 22
linux-source, 22
localepurge, 18
mailman, 32
mailman3, 31
mailman3-full, 32
mailutils, 29
mariadb-server-10.5,galera-4, 34
mdadm, 34
micro-evtd, 11
network-manager, 32
nova-compute, 26
openipmi, 34
openssh-server, 30, 34
openvswitch, 30
popularity-contest, 18
procps, 35
pulseaudio, 35
python-pkg-resources, 34
python-setuptools, 32
rails, 28
rdiff-backup, 29
redmine, 28
release-notes, 1
rsync, 26
rsyslog, 5
sane-airscan, 5
sendmail, 27
slapd, 33
speech-dispatcher, 35
src:gcc-10, 34
src:llvm-toolchain-11, 34
src:qemu, 35
src:squid-deb-proxy, 35
src:wine, 35
src:xen, 35
sshfs, 27
synaptic, 12
systemd, 6
tinc, 11
tpm2-abrmd, 35
udev, 21, 29
unbound, 26
upgrade-reports, 2
usrmerge, 32
vim, 26
vim-addon-manager, 26
vim-scripts, 26
wicd, 32
xfce4-settings, 35
xmlroff, 2
xsltproc, 2
Perl, 4
PHP, 4
Postfix, 4
PostgreSQL, 4

X
Xfce, 3