Notas de lançamento do Debian 11 (bullseye), System z

Projeto de Documentação Debian (https://www.debian.org/doc/)

26 de junho de 2022

Este documento é um software livre; você pode redistribuí-lo e/ou modificá-lo sob os termos da Licença Pública Geral GNU, versão 2, como publicada pela Free Software Foundation.

Este programa é distribuído na expectativa de que seja útil, mas SEM NENHUMA GARANTIA; sem mesmo a garantia implícita de COMERCIABILIDADE ou ADAPTAÇÃO A UM PROPÓSITO PARTICULAR. Veja a Licença Pública Geral GNU (GPL) para mais detalhes.

Você deve ter recebido uma cópia da Licença Pública Geral GNU (GPL) juntamente com este programa; caso contrário, escreva para a Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

O texto da licença também pode ser encontrado em `https://www.gnu.org/licenses/gpl-2.0.html` e no arquivo `/usr/share/common-licenses/GPL-2` em sistemas Debian.

Sumário

1 Introdução **1**
1.1 Reportando bugs neste documento . . . 1
1.2 Contribuindo com relatórios de atualização . . . 1
1.3 Código fonte deste documento . . . 2

2 Quais as novidades no Debian 11 **3**
2.1 Arquiteturas suportadas . . . 3
2.2 Quais as novidades na distribuição? . . . 3
2.2.1 Desktops e pacotes famosos . . . 3
2.2.2 Impressão e escaneamento sem driver . . . 5
2.2.2.1 CUPS e impressão sem driver . . . 5
2.2.2.2 SANE e escaneamento sem driver . . . 5
2.2.3 Novo comando “open” genérico . . . 6
2.2.4 Control groups v2 . . . 6
2.2.5 Journal persistente do systemd . . . 6
2.2.6 Novo método de entrada Fcitx 5 . . . 6
2.2.7 Novidades da Blend Debian Med . . . 6
2.2.8 Suporte do kernel a exFAT . . . 7
2.2.9 Melhorias nas traduções de páginas de manual . . . 7
2.2.10 Melhorias no suporte para sistemas de inicialização alternativos . . . 7

3 Sistema de instalação **9**
3.1 Quais as novidades do sistema de instalação? . . . 9
3.1.1 Ajuda com a instalação de firmware . . . 9
3.1.2 Instalação automatizada . . . 9
3.2 Imagens para Contêineres e Máquinas Virtuais . . . 10

4 Atualizações a partir do Debian 10 (buster) **11**
4.1 Preparando para a atualização . . . 11
4.1.1 Faça backup de quaisquer dados ou informações de configuração . . . 11
4.1.2 Informe os usuários com antecedência . . . 11
4.1.3 Preparar para indisponibilidade de serviços . . . 11
4.1.4 Preparar para recuperação . . . 12
4.1.4.1 Shell de depuração durante a inicialização usando initrd . . . 12
4.1.4.2 Shell de depuração durante a inicialização usando systemd . . . 13
4.1.5 Preparar um ambiente seguro para a atualização . . . 13
4.2 Inicie a partir de um Debian “puro” . . . 13
4.2.1 Atualização para Debian 10 (buster) . . . 13
4.2.2 Remover pacotes não-Debian . . . 14
4.2.3 Atualize para a última versão pontual . . . 14
4.2.4 Prepare o banco de dados de pacotes . . . 14
4.2.5 Remova pacotes obsoletos . . . 14
4.2.6 Remova arquivos de configuração que sobrarem . . . 14
4.2.7 A seção “security” . . . 14
4.2.8 A seção “proposed-updates” . . . 14
4.2.9 Fontes não oficiais . . . 14
4.2.10 Desabilitando o pinning do APT . . . 15
4.2.11 Verifique a situação dos pacotes . . . 15
4.3 Preparando os arquivos source-list do APT . . . 16
4.3.1 Adicionar fontes da Internet ao APT . . . 16
4.3.2 Adicionando fontes ao APT para um espelho local . . . 17
4.3.3 Adicionando fontes ao APT a partir de mídia ótica . . . 17
4.4 Atualizando pacotes . . . 17
4.4.1 Gravando a sessão . . . 18

4.4.2 Atualizando a lista de pacotes . . . 18
4.4.3 Certifique-se que você tem espaço suficiente para a atualização . . . 19
4.4.4 Atualização mínima do sistema . . . 21
4.4.5 Atualizando o sistema . . . 21
4.5 Possíveis problemas durante a atualização . . . 22
4.5.1 O dist-upgrade falha com “Could not perform immediate configuration” . . . 22
4.5.2 Remoções esperadas . . . 22
4.5.3 Loops de conflitos ou pré-dependências . . . 22
4.5.4 Conflitos de arquivo . . . 22
4.5.5 Mudanças de configuração . . . 23
4.5.6 Mudança de sessão para o console . . . 23
4.6 Atualizando o seu kernel e pacotes relacionados . . . 23
4.6.1 Instalando um metapacote do kernel . . . 23
4.7 Preparar para a próxima versão . . . 24
4.7.1 Expurgando pacotes removidos . . . 24
4.8 Pacotes obsoletos . . . 25
4.8.1 Pacotes fictícios transitórios . . . 25

5 Problemas a serem considerados para a bullseye **27**
5.1 Itens específicos da atualização para bullseye . . . 27
5.1.1 O sistema de arquivos XFS não suporta mais a opção barrier/nobarrier . . . 27
5.1.2 Disposição do repositório de seguraça alterada . . . 27
5.1.3 Hash de senha usa yescrypt por padrão . . . 27
5.1.4 Suporte a NSS NIS e NIS+ exige novos pacotes . . . 28
5.1.5 Gerenciamento de fragmentos de arquivos de configuração no “unbound” . . . 28
5.1.6 Obsolescência de parâmetros do rsync . . . 28
5.1.7 Gerenciamento de “addons” do Vim . . . 28
5.1.8 OpenStack e cgroups v1 . . . 28
5.1.9 Arquivos de política da API do OpenStack . . . 29
5.1.10 Indisponibilidade do sendmail durante a atualização . . . 29
5.1.11 FUSE 3 . . . 29
5.1.12 Arquivo de opções do GnuPG . . . 29
5.1.13 Linux habilita espaços de nomes por padrão . . . 29
5.1.14 Linux desabilita chamadas não privilegiadas a bpf() por padrão . . . 30
5.1.15 Redmine faltando na bullseye . . . 30
5.1.16 Exim 4.94 . . . 30
5.1.17 Sondagem de dispositivos SCSI é não determinística . . . 31
5.1.18 rdiff-backup requer atualização sincronizada do servidor e cliente . . . 31
5.1.19 Problemas com microcódigo para CPU Intel . . . 31
5.1.20 Atualizações envolvendo libgc1c2 precisam de duas execuções . . . 31
5.1.21 fail2ban não consegue enviar e-mail usando mail de bsd-mailx . . . 31
5.1.22 Novas conexões SSH não são possíveis durante a atualização . . . 31
5.1.23 Open vSwitch upgrade requires interfaces(5) change . . . 32
5.1.24 Coisas para fazer depois da atualização e antes de reinicializar . . . 32
5.2 Itens não limitados ao processo de atualização . . . 32
5.2.1 Limitações no suporte de segurança . . . 32
5.2.1.1 Situação da segurança dos navegadores web e seus motores de renderização 32
5.2.1.2 OpenJDK 17 . . . 32
5.2.1.3 Pacotes baseados em Go . . . 33
5.2.2 Acessando o aplicativo Configurações do GNOME sem mouse . . . 33
5.2.3 A opção de inicialização `rescue` não é utilizável sem uma senha de root . . . 33
5.3 Obsolescência e depreciação . . . 33
5.3.1 Pacotes obsoletos dignos de nota . . . 33
5.3.2 Componentes obsoletos para a bullseye . . . 34
5.4 Bugs severos conhecidos . . . 35

6 Mais informações sobre o Debian **39**
6.1 Leitura complementar 39
6.2 Obtendo ajuda 39
6.2.1 Listas de discussão 39
6.2.2 Internet Relay Chat 39
6.3 Relatando bugs 39
6.4 Contribuindo para o Debian 40

7 Glossário **41**

A Gerenciando seu sistema buster antes da atualização **43**
A.1 Atualizando seu sistema buster 43
A.2 Verificando seus arquivos source-list do APT 43
A.3 Removendo arquivos de configuração obsoletos 44

B Colaboradores das notas de lançamento **45**

Índice Remissivo **47**

Capítulo 1

Introdução

Este documento dá aos usuários da distribuição Debian informações sobre grandes mudanças na versão 11 (codinome bullseye).

As notas de lançamento fornecem informações sobre como atualizar de forma segura a partir da versão 10 (codinome buster) para a versão atual e dá aos usuários informações sobre potenciais problemas conhecidos que eles possam encontrar nesse processo.

Você pode obter a versão mais recente deste documento em `https://www.debian.org/releases/bullseye/releasenotes`.

> CUIDADO
>
> Note que é impossível listar todos os problemas conhecidos e portanto uma seleção foi feita baseada numa combinação da quantidade esperada e do impacto desses problemas.

Por favor, note que só damos suporte e documentamos a atualização a partir da versão anterior do Debian (nesse caso, a atualização a partir da versão buster). Caso você precise atualizar a partir de versões mais antigas, nós sugerimos que você leia as edições anteriores das notas de lançamento e atualize para a buster primeiro.

1.1 Reportando bugs neste documento

Nós tentamos testar todos os diferentes passos de atualizações descritos neste documento bem como antecipar todos os possíveis problemas que nossos usuários possam encontrar.

Apesar disso, caso você acredite ter encontrado um bug (informação incorreta ou informação que está faltando) nesta documentação, por favor, registre um bug no sistema de rastreamento de bugs (`https://bugs.debian.org/`) para o pacote `release-notes`. É aconselhável que você reveja primeiro os relatórios de bugs existentes (`https://bugs.debian.org/release-notes`) caso a questão que você encontrou já tenha sido relatada. Sinta-se livre para acrescentar informações adicionais aos relatórios de bugs existentes, caso você possa contribuir com conteúdo para este documento.

Apreciamos, e encorajamos, relatórios fornecendo patches para o código fonte deste documento. Você encontrará mais informações sobre como obter o código fonte deste documento na Seção 1.3.

1.2 Contribuindo com relatórios de atualização

Nós apreciamos quaisquer informações dos usuários relacionadas a atualizações da buster para a bullseye. Caso você esteja interessado em compartilhar informação, por favor, registre um bug no sistema de rastreamento de bugs (`https://bugs.debian.org/`) para o pacote `upgrade-reports` com os seus resultados. Nós pedimos que você compacte quaisquer anexos que venha a incluir (usando o **gzip**).

Por favor, inclua as seguintes informações quando enviar seu relatório de atualização:

- O estado da sua base de dados de pacotes antes e depois da atualização: a base de dados de estados do `dpkg` está disponível em `/var/lib/dpkg/status` e a informação do estado dos pacotes do `apt` está disponível em `/var/lib/apt/extended_states`. Você deve ter feito backup antes da atualização conforme descrito na Seção 4.1.1, mas você também pode encontrar backups do `/var/lib/dpkg/status` em `/var/backups`.
- Registros da sessão criados usando o comando **script**, conforme descrito na Seção 4.4.1.
- Seus logs do `apt`, disponíveis em `/var/log/apt/term.log`, ou seus logs do **aptitude**, disponíveis em `/var/log/aptitude`.

NOTA

Você deve usar algum tempo para revisar e remover qualquer informação sensível e/ou confidencial dos logs antes de incluí-los no relatório de bug, pois a informação será disponibilizada em um banco de dados público.

1.3 Código fonte deste documento

O código fonte deste documento está no formato DocBook XML. A versão HTML é gerada usando `docbook-xsl` e `xsltproc`. A versão PDF é gerada usando `dblatex` ou `xmlroff`. Os códigos fonte das notas de lançamento estão disponíveis no repositório Git do *Projeto de Documentação Debian*. Você pode usar a interface web (`https://salsa.debian.org/ddp-team/release-notes/`) para acessar seus arquivos individualmente através da web e ver suas mudanças. Para mais informações sobre como acessar o Git, por favor, consulte as páginas de informação sobre VCS do Projeto de Documentação Debian (`https://www.debian.org/doc/vcs`).

Capítulo 2

Quais as novidades no Debian 11

O Wiki (`https://wiki.debian.org/NewInBullseye`) contém mais informações sobre esse tópico.

2.1 Arquiteturas suportadas

As seguintes arquiteturas são oficialmente suportadas pelo Debian 11:

- PC de 32 bits (“i386”) e PC de 64 bits (“amd64”)
- ARM 64 bits (“arm64”)
- ARM EABI (`armel`)
- ARMv7 (EABI com unidade de ponto flutuante ABI, “armhf”)
- little-endian MIPS (`mipsel`)
- 64-bit little-endian MIPS (“mips64el”)
- PowerPC little-endian 64 bits (`ppc64el`)
- IBM System z (`s390x`)

Você pode ler mais sobre o estado dos portes e informações específicas sobre o porte para sua arquitetura nas páginas web dos portes Debian (`https://www.debian.org/ports/`).

2.2 Quais as novidades na distribuição?

Esta nova versão do Debian vem novamente com muito mais software do que seu antecessor buster; a distribuição inclui mais de 11294 novos pacotes, de um total de mais de 59551 pacotes. A maioria do software da distribuição foi atualizada: mais de 42821 pacotes de software (isso é 72% de todos os pacotes no buster). Além disso, um número significativo de pacotes (mais de 9519, 16% dos pacotes no buster) foram, por várias razões, removidos da distribuição. Você não verá atualizações para esses pacotes e eles serão marcados como ”obsoletos” nas interfaces de gerenciamento de pacotes; veja Seção 4.8.

2.2.1 Desktops e pacotes famosos

O Debian mais uma vez vem com vários aplicativos e ambientes de área de trabalho. Entre outros, agora inclui os ambientes de área de trabalho GNOME 3.38, KDE Plasma 5.20, LXDE 11, LXQt 0.16, MATE 1.24, e Xfce 4.16.

Os aplicativos de produtividade também foram atualizados, incluindo as suítes de escritório:

- O LibreOffice está atualizado para a versão 7.0;
- O Calligra está atualizado para 3.2;

- O GNUcash está atualizado para 4.4;

Entre várias outras, esta versão também inclui as seguintes atualizações de software:

Pacote	Versão no 10 (buster)	Versão no 11 (bullseye)
Apache	2.4.38	2.4.48
Servidor DNS BIND	9.11	9.16
Cryptsetup	2.1	2.3
Dovecot MTA	2.3.4	2.3.13
Emacs	26.1	27.1
Exim servidor de e-mail padrão	4.92	4.94
GNU Compiler Collection (Coleção de Compiladores GNU) como compilador padrão	8.3	10.2
GIMP	2.10.8	2.10.22
GnuPG	2.2.12	2.2.27
Inkscape	0.92.4	1.0.2
a biblioteca GNU C	2.28	2.31
lighttpd	1.4.53	1.4.59
imagem do kernel Linux	série 4.19	série 5.10
Cadeia base de ferramentas LLVM/Clang	6.0.1 e 7.0.1 (padrão)	9.0.1 e 11.0.1 (padrão)
MariaDB	10.3	10.5
Nginx	1.14	1.18
OpenJDK	11	11
OpenSSH	7.9p1	8.4p1
Perl	5.28	5.32
PHP	7.3	7.4
Postfix MTA	3.4	3.5
PostgreSQL	11	13
Python 3	3.7.3	3.9.1
Rustc	1.41 (1.34 para `armel`)	1.48
Samba	4.9	4.13
Vim	8.1	8.2

2.2.2 Impressão e escaneamento sem driver

Tanto imprimir com `CUPS` quanto escanear com `SANE` está se tornando cada vez mais possível sem a necessidade de qualquer driver (muitas vezes não livre) específico para o modelo do equipamento, especialmente no caso de dispositivos que entraram no mercado nos últimos cinco anos aproximadamente.

2.2.2.1 CUPS e impressão sem driver

Impressoras modernas conectadas por rede ethernet ou sem fio já podem usar impressão sem driver (`https://wiki.debian.org/CUPSQuickPrintQueues`), implementada via `CUPS` e `cups-filters`, como descrito nas Notas de Lançamento para buster (`https://www.debian.org/releases/buster/amd64/release-notes/ch-whats-new.html#driverless-printing`). O Debian 11 "bullseye" trás o novo pacote `ipp-usb`, que é recomendado por `cups-daemon` e usa o protocolo independente de fornecedor IPP-over-USB (`https://wiki.debian.org/CUPSDriverlessPrinting#ippoverusb`) que encontra suporte em várias impressoras modernas. Isso permite que um dispositivo USB seja tratado como um dispositivo de rede, estendendo a impressão sem driver para incluir impressoras conectadas via USB. Os detalhes estão descritos no wiki (`https://wiki.debian.org/CUPSDriverlessPrinting#ipp-usb`).

O arquivo de serviço do systemd incluído no pacote `ipp-usb` inicia o daemon `ipp-usb` quando uma impressora é conectada via USB, dessa forma tornando-a disponível para impressão. Por padrão, `cups-browsed` deve configurá-la automaticamente, ou ela pode ser configurada manualmente com uma fila de impressão local sem driver (`https://wiki.debian.org/SystemPrinting`).

2.2.2.2 SANE e escaneamento sem driver

O suporte sem driver oficial `SANE` é provido por `sane-escl` no `libsane1`. Um suporte sem driver desenvolvido de forma independente é o `sane-airscan`. Os dois suportes entendem o protocolo eSCL (`https://wiki.debian.org/SaneOverNetwork#escl`), mas `sane-airscan` também pode usar

o protocolo WSD (https://wiki.debian.org/SaneOverNetwork#wsd). Usuários devem considerar ter os dois suportes em seu sistema.

eSCL e WSD são protocolos de rede. Consequentemente, eles vão operar através de uma conexão USB se o dispositivo for IPP-over-USB (veja acima). Note que libsane1 tem ipp-usb como um pacote recomendado. Isto faz com que um dispositivo compatível seja automaticamente configurado para usar um suporte sem driver quando conectado a uma porta USB.

2.2.3 Novo comando "open" genérico

Um novo comando **open** está disponível como um alias de conveniência para **xdg-open** (por padrão) ou **run-mailcap**, gerenciado pelo sistema update-alternatives(1) (https://manpages.debian.org//bullseye/dpkg/update-alternatives.1.html). Ele é projetado para o uso interativo na linha de comando, para abrir arquivos usando seus respectivos aplicativos padrão, os quais podem ser programas gráficos, quando disponíveis.

2.2.4 Control groups v2

Na bullseye, o systemd usa por padrão "control groups v2" (cgroupv2), o qual fornece uma hierarquia unificada de controle de recursos. Parâmetros de linha de comando do kernel estão disponíveis para reabilitar os cgroups legados, se necessário. Veja as notas para o OpenStack na Seção 5.1.8.

2.2.5 Journal persistente do systemd

O systemd no bullseye ativa a sua funcionalidade de journal persistente por padrão, armazenando os seus arquivos em /var/log/journal/. Veja systemd-journald.service(8) (https://manpages.debian.org//bullseye/systemd/systemd-journald.service.8.html) para detalhes; note que no Debian o journal pode ser lido por membros do grupo adm, em adição ao grupo padrão systemd-journal.

Isso não deve interferir com qualquer daemon de log tradicional existente, tal como rsyslog, mas usuários que não estejam dependendo de quaisquer características especiais de tal daemon podem querer desinstalá-lo e passar a usar somente o journal.

2.2.6 Novo método de entrada Fcitx 5

O Fcitx 5 é um método de entrada para os idiomas Chinês, Japonês, Coreano e muitos outros. Ele é o sucessor do popular Fcitx 4 na buster. A nova versão tem suporte a Wayland e melhor suporte a módulos adicionais. Mais informação, incluindo o guia de migração, pode ser encontrada no wiki (https://wiki.debian.org/I18n/Fcitx5).

2.2.7 Novidades da Blend Debian Med

A equipe Debian Med tem feito parte da luta contra a COVID-19, empacotando software para pesquisa do vírus a nível de sequência e para combater a pandemia com as ferramentas usadas em epidemiologia. O esforço continuará no próximo ciclo de lançamento, com foco em ferramentas de aprendizado de máquina que são usadas em ambos os campos.

Além da adição de novos pacotes no campo das ciências da vida e medicina, mais e mais pacotes existentes ganharam suporte a Integração Contínua.

Uma gama de aplicações de desempenho crítico agora se beneficia de SIMD Everywhere (https://wiki.debian.org/SIMDEverywhere). Essa biblioteca permite que pacotes sejam disponibilizados em mais plataformas de hardware suportadas pelo Debian (notavelmente, em arm64) ao mesmo tempo em que mantém o benefício de desempenho trazido por processadores com suporte a extensões de vetor, tais como AVX em amd64, ou NEON em arm64.

Para instalar os pacotes mantidos pela equipe Debian Med, instale os meta pacotes denominados med-*, que estão na versão 3.6.x para o Debian bullseye. Sinta-se livre para visitar as páginas de tarefas Debian Med (https://blends.debian.org/med/tasks) para ver a gama completa de software biológico e médico disponível no Debian.

2.2.8 Suporte do kernel a exFAT

Bullseye é o primeiro lançamento a fornecer um kernel Linux com suporte ao sistema de arquivos exFAT e, por padrão, usa tal suporte para montar sistemas de arquivos desse tipo. Consequentemente, não é mais necessário usar a implementação de sistema de arquivos em espaço de usuário fornecida pelo pacote `exfat-fuse`. Se você gostaria de continuar a usar a implementação de sistema de arquivos em espaço de usuário, você precisa invocar o comando auxiliar **mount.exfat-fuse** diretamente ao montar um sistema de arquivos exFAT.

Ferramentas para criar e checar um sistema de arquivos exFAT são fornecidas pelo pacote `exfatprogs` pelos autores da implementação exFAT do kernel Linux. A implementação independente dessas ferramentas fornecida pelo pacote existente `exfat-utils` ainda está disponível, mas não pode ser instalada simultaneamente com a nova implementação. É recomendado migrar para o pacote `exfatprogs`, embora você deva tomar cuidado com as opções de comando, as quais são provavelmente incompatíveis.

2.2.9 Melhorias nas traduções de páginas de manual

As páginas de manual para diversos projetos, tais como systemd, util-linux, OpenSSH e Mutt, em várias línguas, incluindo francês, espanhol e macedônio, foram melhoradas substancialmente. Para se beneficiar disso, por favor, instale `manpages-xx` (onde `xx` é o código para a sua língua natural preferida).

Durante o tempo de vida da versão bullseye, "backports" de melhorias adicionais na tradução serão fornecidas através do repositório `backports`.

2.2.10 Melhorias no suporte para sistemas de inicialização alternativos

O sistema de inicialização padrão no Debian é o `systemd`. Na bullseye, uma quantidade de sistemas de inicialização alternativos são suportados (tais como inicialização no estilo System-V e OpenRC), e a maioria dos ambientes de área de trabalho agora funcionam bem em sistemas executando inicializações alternativas. Detalhes sobre como trocar o sistema de inicialização (e onde encontrar ajuda com problemas relacionados a executar outras inicializações diferentes do systemd) estão disponíveis na wiki do Debian (`https://wiki.debian.org/Init`).

Capítulo 3

Sistema de instalação

O Instalador Debian é o sistema de instalação oficial para o Debian. Ele oferece vários métodos de instalação. Os métodos disponíveis para instalar seu sistema dependem da sua arquitetura.

Imagens do instalador para a bullseye podem ser encontradas juntamente com o Guia de Instalação no site web do Debian (`https://www.debian.org/releases/bullseye/debian-installer/`).

O Guia de Instalação também está incluído na primeira mídia dos conjuntos de DVDs (CDs/blu-rays) oficiais do Debian, disponíveis em:

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

Também pode ser do seu interesse verificar a errata (`https://www.debian.org/releases/bullseye/debian-installer/index#errata`) do debian-installer que contém uma lista de problemas conhecidos.

3.1 Quais as novidades do sistema de instalação?

Muito desenvolvimento foi feito no Instalador Debian desde seu lançamento oficial anterior com o Debian 10, resultando em melhorias no suporte a hardware e em alguns novos recursos ou melhorias muito interessantes.

Caso você esteja interessado nas mudanças detalhadas desde a buster, por favor, verifique os anúncios de lançamento das versões beta e RC da bullseye disponíveis a partir do histórico de notícias (`https://www.debian.org/devel/debian-installer/News/`) do Instalador Debian.

3.1.1 Ajuda com a instalação de firmware

Cada vez mais, dispositivos periféricos requerem que seja carregado firmware como parte da inicialização do hardware. Para ajudar a lidar com esse problema, o instalador tem uma nova funcionalidade. Se algum hardware instalado requer arquivos de firmware para a sua instalação, o instalador tentará adicioná-los ao sistema, baseado em um mapeamento do ID do hardware com os nomes dos arquivos de firmware.

Essa nova funcionalidade é restrita às imagens não oficiais do instalador com firmware incluído (veja https://www.debian.org/releases/bullseye/debian-installer/#firmware_nonfree (`https://www.debian.org/releases/bullseye/debian-installer/#firmware_nonfree`)). Geralmente, o firmware não está em conformidade com a DFSG, por isso, não é possível distribuí-lo pelo repositório "main" do Debian.

Se você enfrentar problemas relacionados a firmware (em falta), por favor, leia o capítulo dedicado a isso no guia de instalação (`https://www.debian.org/releases/bullseye/amd64/ch06s04#completing-installed-system`).

3.1.2 Instalação automatizada

Algumas mudanças também implicam em mudanças no suporte do instalador para instalação automatizada utilizando arquivos de pré configuração. Isso significa que, caso você tenha arquivos de confi-

guração preexistentes que funcionaram com o instalador da buster, você não pode esperar que esses funcionem com o novo instalador sem modificação.

O Guia de Instalação (`https://www.debian.org/releases/bullseye/installmanual`) possui um apêndice atualizado separado com uma extensa documentação sobre como usar a pré configuração.

3.2 Imagens para Contêineres e Máquinas Virtuais

Imagens multi arquitetura do Debian bullseye para contêineres estão disponíveis no Docker Hub (`https://hub.docker.com/_/debian`). Em adição às imagens padrão, está disponível uma variante "slim" que reduz o uso de disco.

Imagens para máquinas virtuais para o gerenciador de VM "Hashicorp Vagrant" estão publicadas em Vagrant Cloud (`https://app.vagrantup.com/debian`).

Capítulo 4

Atualizações a partir do Debian 10 (buster)

4.1 Preparando para a atualização

Nós sugerimos que antes de atualizar você também leia as informações em Capítulo 5. Esse capítulo aborda potenciais problemas, os quais não estão diretamente relacionados ao processo de atualização, mas que ainda pode ser importante conhecer antes que você comece.

4.1.1 Faça backup de quaisquer dados ou informações de configuração

Antes de atualizar o seu sistema, é fortemente recomendado que você faça um backup completo ou, pelo menos, faça backup de quaisquer dados ou informações de configuração que você não possa perder. As ferramentas de atualização e o processo são bastante confiáveis, mas uma falha de hardware no meio de uma atualização pode resultar em um sistema severamente danificado.

Os principais dados que você terá que fazer backup são os conteúdos do `/etc`, `/var/lib/dpkg`, `/var/lib/apt/extended_states` e a saída do `dpkg --get-selections "*"` (as aspas são importantes). Caso você utilize o **aptitude** para gerenciar pacotes em seu sistema, você também terá que fazer backup do `/var/lib/aptitude/pkgstates`.

O processo de atualização em si não modifica nada no diretório `/home`. Porém, alguns aplicativos (por exemplo, partes da suíte Mozilla e os ambientes de área de trabalho GNOME e KDE) são conhecidos por sobrescrever as configurações existentes dos usuários com novos padrões, quando uma nova versão do aplicativo é iniciada pela primeira vez por um usuário. Como precaução, você pode fazer um backup dos arquivos e diretórios ocultos ("dotfiles") nos diretórios home dos usuários. Esse backup pode ajudar a recuperar ou recriar antigas configurações. Você também pode informar os usuários sobre isso.

Qualquer operação de instalação de pacote deve ser executada com privilégios de superusuário, para isso, faça login como `root` ou use o **su** ou o **sudo** para obter os direitos de acesso necessários.

A atualização possui algumas condições prévias; você deve verificá-las antes de começar a executar a atualização.

4.1.2 Informe os usuários com antecedência

É sensato informar a todos os usuários com antecedência sobre qualquer atualização que você esteja planejando, embora os usuários que acessem o seu sistema via uma conexão **ssh** pouco devam notar durante a atualização, e devam ser capazes de continuar trabalhando.

Caso você deseje tomar precauções extras, faça backup ou desmonte a partição `/home` antes de atualizar.

Você terá que fazer uma atualização de kernel quando atualizar para o bullseye, então, uma reinicialização será necessária. Normalmente, isso será feito depois que a atualização for concluída.

4.1.3 Preparar para indisponibilidade de serviços

Poderão haver serviços que são oferecidos pelo sistema que estão associados aos pacotes que serão incluídos na atualização. Se esse for o caso, por favor, note que durante a atualização esses serviços

serão interrompidos, enquanto os seus pacotes associados estiverem sendo substituídos e configurados. Durante esse tempo, esses serviços não estarão disponíveis.

O tempo exato de indisponibilidade desses serviços variará dependendo do número de pacotes sendo atualizados no sistema, e isso também inclui o tempo que o administrador do sistema gasta respondendo a quaisquer perguntas de configuração das atualizações dos pacotes. Observe que, se o processo de atualização for deixado sem acompanhamento e o sistema solicitar uma entrada durante a atualização, existe uma grande possibilidade dos serviços ficarem indisponíveis[1] por um período significativo de tempo.

Se o sistema que está sendo atualizado fornecer serviços críticos para os seus usuários ou para a rede[2], você pode reduzir o tempo de indisponibilidade caso você faça uma atualização mínima do sistema, como descrito em Seção 4.4.4, seguida de uma atualização do kernel e reinicialização, e então atualizar os pacotes associados aos seus serviços críticos. Atualize esses pacotes antes de fazer a atualização completa descrita em Seção 4.4.5. Dessa forma, você pode garantir que esses serviços essenciais estejam funcionando e disponíveis durante o processo de atualização completa, e o seu tempo de indisponibilidade é reduzido.

4.1.4 Preparar para recuperação

Embora o Debian tente garantir que o seu sistema permaneça inicializável a todo o momento, sempre há uma chance de você ter problemas ao reinicializar o seu sistema após a atualização. Problemas possíveis conhecidos são documentados neste e nos próximos capítulos destas notas de lançamento.

Por essa razão faz sentido garantir que você seja capaz de recuperar o seu sistema caso não consiga reinicializar ou, para sistemas gerenciados remotamente, não consiga levantar a rede.

Caso você esteja atualizando remotamente através de um link **ssh**, é recomendado que você tome as precauções necessárias para ser capaz de acessar o servidor por meio de um terminal serial remoto. Há uma chance de que, após atualizar o kernel e reinicializar, você tenha que corrigir a configuração do sistema por meio de um console local. Além disso, se o sistema for reinicializado acidentalmente no meio de uma atualização, existe uma chance de que você precise recuperá-lo usando um console local.

Para recuperação de emergência, nós geralmente recomendamos usar o *modo de recuperação* do Instalador Debian da bullseye. A vantagem de usar o instalador é que você pode escolher entre os seus vários métodos para encontrar aquele que melhor se adéqua à sua situação. Para mais informações, por favor, consulte a seção "Recuperando um sistema quebrado" no capítulo 8 do Guia de Instalação (`https://www.debian.org/releases/bullseye/installmanual`) e a FAQ do Instalador Debian (`https://wiki.debian.org/DebianInstaller/FAQ`).

Se isso falhar, você precisará de uma forma alternativa de inicializar seu sistema, e assim poder acessá-lo e repará-lo. Uma opção é usar uma imagem especial de recuperação ou de instalação "live" (`https://www.debian.org/CD/live/`). Após a inicialização a partir dela, você deverá ser capaz de montar o seu sistema de arquivos raiz e fazer **chroot** nele para investigar e corrigir o problema.

4.1.4.1 Shell de depuração durante a inicialização usando initrd

O pacote `initramfs-tools` inclui um shell de depuração[3] nas initrds que ele gera. Se, por exemplo, a initrd for incapaz de montar o seu sistema de arquivos raiz, você será deixado nesse shell de depuração que tem comandos básicos disponíveis para ajudar a rastrear o problema e possivelmente corrigi-lo.

Coisas básicas a serem verificadas: presença dos arquivos de dispositivo corretos em `/dev`; quais módulos estão carregados (`cat /proc/modules`); saída do **dmesg** com erros de carregamento de drivers. A saída do **dmesg** também exibirá quais arquivos de dispositivo foram associados a quais discos; você deve verificar isso com a saída do `echo $ROOT` para certificar-se que o sistema de arquivos raiz está no dispositivo esperado.

Caso você consiga resolver o problema, digitando `exit` sairá do shell de depuração e continuará o processo de inicialização a partir do ponto em que ele falhou. Claro que você também precisará corrigir a causa do problema e gerar novamente a initrd, pois assim a próxima inicialização não falhará novamente.

[1] Se a prioridade do debconf estiver configurada em um nível muito alto, você pode evitar perguntas de configuração, mas os serviços que dependam de respostas predefinidas que não são aplicáveis aos seu sistema falharão ao iniciar.

[2] Por exemplo: serviços de DNS ou DHCP, especialmente quando não há redundância ou substituto em caso de falha ("failover"). No caso do DHCP, os usuários finais poderão ser desconectados da rede se o tempo de concessão ("lease time") for menor do que o tempo que leva para completar o processo de atualização.

[3] Esse recurso pode ser desabilitado adicionando o parâmetro `panic=0` aos seus parâmetros de inicialização.

4.1.4.2 Shell de depuração durante a inicialização usando systemd

No caso da inicialização falhar sob o systemd, é possível obter um shell root de depuração alterando-se a linha de comando do kernel. Caso a inicialização básica funcione, mas alguns dos serviços falhem ao iniciar, pode ser útil adicionar `systemd.unit=rescue.target` aos parâmetros do kernel.

Caso contrário, o parâmetro do kernel `systemd.unit=emergency.target` irá fornecer-lhe um shell root no momento mais imediato possível. Porém, isso é feito antes da montagem do sistema de arquivos raiz com permissões de leitura e escrita. Você terá que fazer isso manualmente com:

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

Mais informações sobre depuração de uma inicialização quebrada sob systemd podem ser encontradas no artigo Diagnosticando problemas de inicialização (`https://freedesktop.org/wiki/Software/systemd/Debugging/`).

4.1.5 Preparar um ambiente seguro para a atualização

IMPORTANTE

Caso você esteja usando alguns serviços VPN (tais como `tinc`), considere que eles podem não estar disponíveis ao longo do processo de atualização. Por favor, veja Seção 4.1.3.

A fim de conseguir uma margem extra de segurança quando atualizar remotamente, nós sugerimos que você execute o processo de atualização no console virtual fornecido pelo programa **screen**, que permite uma reconexão segura e garante que o processo de atualização não seja interrompido mesmo se o processo de conexão remota falhar temporariamente.

4.2 Inicie a partir de um Debian "puro"

O processo de atualização descrito neste capítulo foi projetado para sistemas Debian estáveis "puros". O APT controla o que é instalado no seu sistema. Se a sua configuração do APT faz menção a fontes adicionais além da buster, ou se você tiver pacotes instalados de outros lançamentos ou de terceiros, então para garantir um processo de atualização confiável, talvez você queira iniciar removendo esses fatores de complicação.

O principal arquivo de configuração que o APT usa para decidir de quais fontes ele deve baixar pacotes é `/etc/apt/sources.list`, mas ele também pode usar arquivos do diretório `/etc/apt/sources.list.d/` - para detalhes, veja sources.list(5) (`https://manpages.debian.org/bullseye/apt/sources.list.5.html`). Se o seu sistema estiver usando múltiplos arquivos sourcelist, então você precisa garantir que eles estejam consistentes.

4.2.1 Atualização para Debian 10 (buster)

Atualizações diretas a partir de versões do Debian mais antigas do que a 10 (buster) não são suportadas. Veja a sua versão do Debian com:

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

Por favor, siga as instruções nas Notas de lançamento para Debian 10 (`https://www.debian.org/releases/buster/releasenotes`) para atualizar para Debian 10 primeiro.

4.2.2 Remover pacotes não-Debian

Abaixo, há dois métodos para encontrar pacotes instalados que não foram fornecidos pelo Debian, usando **aptitude** ou **apt-forktracer**. Por favor, note que nenhum deles é 100% preciso (por exemplo: o método usando aptitude listará pacotes que já foram fornecidos pelo Debian no passado, mas não são mais, tais como pacotes de kernels antigos).

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

4.2.3 Atualize para a última versão pontual

Esse procedimento assume que o seu sistema foi atualizado para a versão pontual mais recente do buster. Caso você não tenha feito isso ou não tenha certeza, siga as instruções em Seção A.1.

4.2.4 Prepare o banco de dados de pacotes

Você deve se certificar de que o banco de dados de pacotes esteja pronto antes de continuar com a atualização. Se você for um usuário de outro gerenciador de pacotes, como `aptitude` ou `synaptic`, revise quaisquer ações pendentes. Um pacote agendado para instalação ou remoção pode interferir no procedimento de atualização. Note que só é possível corrigir isso se os seus arquivos source-list do APT ainda apontarem para *buster* e não para *stable* ou *bullseye*; veja Seção A.2.

4.2.5 Remova pacotes obsoletos

É uma boa ideia remover pacotes obsoletos do seu sistema antes da atualização. Eles podem introduzir complicações durante o processo de atualização e podem apresentar riscos de segurança pois não são mais mantidos.

4.2.6 Remova arquivos de configuração que sobrarem

Uma atualização anterior pode ter deixado cópias não usadas de arquivos de configuração; versões antigas de arquivos de configuração, versões fornecidas pelos mantenedores dos pacotes, etc. Remover arquivos que sobraram de atualizações anteriores pode evitar confusão. Encontre esses arquivos que sobraram com:

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

4.2.7 A seção "security"

Para linhas de fontes do APT que referenciam o repositório "security", o formato mudou um pouco junto ao nome da versão, indo de `buster/updates` para `bullseye-security`; veja Seção 5.1.2.

4.2.8 A seção "proposed-updates"

Caso você tenha a seção `proposed-updates` presente nos seus arquivos source-list do APT, você deve removê-la antes de tentar atualizar o seu sistema. Essa é uma precaução para reduzir a probabilidade de conflitos.

4.2.9 Fontes não oficiais

Caso você tenha quaisquer pacotes não-Debian no seu sistema, você deve estar ciente de que esses podem ser removidos durante a atualização por causa de dependências conflitantes. Se esses pacotes foram instalados pela adição de um repositório extra nos seus arquivos source-list do APT, você deve verificar se tal repositório também oferece pacotes compilados para bullseye e alterar o item da fonte adequadamente ao mesmo tempo que alterar os seus itens das fontes para os pacotes Debian.

Alguns usuários podem ter versões atualizadas retroativamente ("backported") *não-oficiais* "mais novas" dos pacotes que *estão* no Debian instaladas no seu sistema buster. Tais pacotes são mais prováveis de causar problemas durante a atualização, pois podem resultar em conflitos de arquivo[4]. Seção 4.5 tem algumas informações sobre como lidar com conflitos de arquivo caso eles ocorram.

4.2.10 Desabilitando o pinning do APT

Caso você tenha configurado o APT para instalar determinados pacotes a partir de uma distribuição diferente da "stable" (por exemplo, da "testing"), você pode ter que mudar sua configuração de pinning do APT (guardada em `/etc/apt/preferences` e `/etc/apt/preferences.d/`) para permitir a atualização dos pacotes para as versões existentes na nova versão "stable". Mais informações sobre pinning do APT podem ser encontradas em apt_preferences(5) (`https://manpages.debian.org/bullseye/apt/apt_preferences.5.en.html`).

4.2.11 Verifique a situação dos pacotes

Independentemente do método usado para atualização, é recomendado que você primeiro verifique a situação de todos os pacotes, e verifique se todos estão em uma situação atualizável. O seguinte comando exibirá quaisquer pacotes que tenham uma situação de "Half-Installed" ou "Failed-Config", e aqueles com alguma situação de erro.

```
# dpkg --audit
```

Você também pode inspecionar o estado de todos os pacotes em seu sistema utilizando o **aptitude** ou com comandos como

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

ou

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

É desejável remover quaisquer retenções (holds) em pacotes antes da atualização. Se qualquer pacote que seja essencial para a atualização estiver retido, a atualização falhará.

Note que o **aptitude** usa um método para registrar os pacotes que estão retidos diferente do **apt** e do **dselect**. Você pode identificar pacotes retidos pelo **aptitude** com

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

Caso você queira verificar quais pacotes você tem retidos pelo **apt**, você deve usar

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

Se você alterou e recompilou um pacote localmente, e não o renomeou ou colocou uma época na versão, você deve colocá-lo em retenção para evitar que seja atualizado.

O estado do pacote em "hold" pelo **apt** pode ser alterado usando:

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

Substitua `hold` por `install` para remover o estado de "hold".

Se existir alguma coisa que você precise corrigir, é melhor certificar-se que os seus arquivos source-list do APT ainda se refiram a buster, como explicado em Seção A.2.

[4] O sistema de gerenciamento de pacotes do Debian normalmente não permite que um pacote remova ou atualize um arquivo pertencente a outro pacote, a menos que ele tenha sido definido para substituir esse pacote.

4.3 Preparando os arquivos source-list do APT

Antes de iniciar a atualização, você deve reconfigurar os arquivos source-list do APT (`/etc/apt/sources.list` e arquivos sob `/etc/apt/sources.list.d/`) para adicionar fontes para `bullseye` e, geralmente, remover fontes para `buster`.

O APT considerará todos os pacotes que possam ser encontrados através de qualquer repositório configurado e instalará o pacote com o número de versão mais elevado, dando prioridade à primeira entrada encontrada nos arquivos. Assim, se você tiver múltiplas localizações de espelhos, liste primeiro os que estiverem em discos rígidos locais, depois CD-ROMs, e então os espelhos remotos.

Uma versão pode normalmente ser referida tanto pelo seu codinome (por exemplo, `buster`, `bullseye`) como pelo seu nome de estado (ou seja, `oldstable`, `stable`, `testing`, `unstable`). Referir-se a uma versão pelo seu codinome tem a vantagem que você nunca será surpreendido por uma nova versão, e por essa razão essa abordagem é adotada aqui. Isso significa certamente que você mesmo terá que ficar atento aos anúncios de lançamento. Caso você use o nome de estado em vez disso, apenas verá grandes quantidades de atualizações dos pacotes disponíveis assim que um lançamento acontecer.

O Debian fornece duas listas de e-mail de anúncios para ajudar você a ficar atualizado sobre informações relevantes relacionadas a lançamentos do Debian:

- Ao se inscrever na lista de e-mail de anúncios do Debian (`https://lists.debian.org/debian-announce/`), você receberá uma notificação a cada vez que o Debian fizer um novo lançamento. Tal como quando a `bullseye` trocar de, por exemplo, `testing` para `stable`.

- Ao se inscrever na lista de e-mail de anúncios de segurança do Debian (`https://lists.debian.org/debian-security-announce/`), você receberá uma notificação a cada vez que o Debian publicar um anúncio de segurança.

4.3.1 Adicionar fontes da Internet ao APT

Em novas instalações, o padrão é que o APT seja configurado para usar o serviço de CDN para APT do Debian, o qual deve assegurar que os pacotes sejam automaticamente baixados de um servidor próximo de você em termos de rede. Como esse é um serviço relativamente novo, instalações antigas podem ter configurações que ainda apontam para algum dos servidores de Internet principais do Debian ou algum dos seus espelhos. Se você ainda não o fez, é recomendado passar a usar o serviço de CDN na sua configuração do APT.

Para fazer uso do serviço de CDN, adicione uma linha como esta na sua configuração de fonte do APT (assumindo que você esteja usando `main` e `contrib`):

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

Após adicionar suas novas fontes, desabilite as linhas "`deb`" previamente existentes pondo um sinal de cerquilha (`#`) no início delas.

No entanto, se você obtiver melhores resultados usando um espelho específico que seja mais próximo de você em termos de rede, essa opção ainda está disponível.

Os endereços dos espelhos do Debian podem ser encontrados em `https://www.debian.org/distrib/ftplist` (veja na seção "lista de espelhos do Debian").

Por exemplo, suponha que seu espelho Debian mais próximo seja `http://mirrors.kernel.org`. Se você examinar esse espelho com um navegador web, você notará que os diretórios principais estão organizados assim:

```
http://mirrors.kernel.org/debian/dists/bullseye/main/binary-s390x/...
http://mirrors.kernel.org/debian/dists/bullseye/contrib/binary-s390x/...
```

Para configurar o APT para usar um determinado espelho, adicione uma linha como esta (novamente, assumindo que você esteja usando `main` e `contrib`):

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

Note que o "`dists`" é adicionado implicitamente, e os argumentos após o nome da versão são usados para expandir o caminho em múltiplos diretórios.

Novamente, depois de adicionar as suas novas fontes, desabilite as entradas de repositórios previamente existentes.

4.3.2 Adicionando fontes ao APT para um espelho local

Em vez de usar espelhos de pacotes remotos, é possível que você deseje modificar os arquivos source-list do APT para usar um espelho em um disco local (possivelmente montado sobre NFS).

Por exemplo, seu espelho de pacotes pode estar sob `/var/local/debian/`, e ter diretórios principais assim:

```
/var/local/debian/dists/bullseye/main/binary-s390x/...
/var/local/debian/dists/bullseye/contrib/binary-s390x/...
```

Para usar isso com o `apt`, adicione esta linha ao seu arquivo `sources.list`:

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

Note que o "`dists`" é adicionado implicitamente, e os argumentos após o nome da versão são usados para expandir o caminho em múltiplos diretórios.

Após adicionar suas novas fontes, desabilite as entradas de repositórios previamente existentes em arquivos source-list do APT pondo um sinal de cerquilha (`#`) no início delas.

4.3.3 Adicionando fontes ao APT a partir de mídia ótica

Caso você queira usar *somente* DVDs (ou mídias de CD ou Blu-ray), comente as entradas já existentes em todos os arquivos source-list do APT pondo um sinal de cerquilha (`#`) no início delas.

Certifique-se de que existe uma linha em `/etc/fstab` que habilite a montagem do seu drive de CD-ROM no ponto de montagem `/media/cdrom`. Por exemplo, caso `/dev/sr0` seja o seu drive de CD-ROM, o `/etc/fstab` deve conter uma linha como:

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

Note que não deve haver *nenhum espaço* entre as palavras `noauto,ro` no quarto campo.

Para verificar se funciona, insira um CD e tente executar

```
# mount /media/cdrom    # isso montará o CD no ponto de montagem
# ls -alF /media/cdrom  # isso deverá exibir o diretório raiz do CD
# umount /media/cdrom   # isso desmontará o CD
```

Depois, execute:

```
# apt-cdrom add
```

para cada CD-ROM de binários do Debian que você tiver, para adicionar os dados a respeito de cada CD à base de dados do APT.

4.4 Atualizando pacotes

A forma recomendada para atualizar a partir de versões anteriores do Debian é usar a ferramenta de gerenciamento de pacotes **apt**.

NOTA

O **apt** é indicado para uso interativo, e não deve ser usado em scripts. Em scripts, deve-se usar **apt-get**, o qual tem uma saída estável mais apropriada para análise.

Não esqueça de montar todas as partições necessárias (especialmente as partições raiz e `/usr`) com permissões de leitura e escrita, com um comando como:

```
# mount -o remount,rw /ponto-de-montagem
```

Em seguida, você deve confirmar novamente se as entradas das fontes do APT (em `/etc/apt/sources.list` e nos arquivos sob `/etc/apt/sources.list.d/`) referem-se a "`bullseye`" ou a "`stable`". Não devem haver quaisquer entradas de fontes que apontem para buster

NOTA

As linhas de fontes de um CD-ROM podem às vezes se referir à "`unstable`"; embora isso possa ser confuso, você *não* deve alterá-las.

4.4.1 Gravando a sessão

É fortemente recomendado que você utilize o programa **/usr/bin/script** para gravar uma transcrição da sessão de atualização. Então, se um problema ocorrer, você terá um registro do que aconteceu e, se necessário, poderá fornecer informações precisas em um relatório de bug. Para iniciar a gravação, digite:

```
# script -t 2>~/upgrade-bullseye-etapa.hora -a ~/upgrade-bullseye-etapa.script
```

ou semelhante. Caso você tenha que reexecutar a transcrição (por exemplo, caso você tenha que reinicializar o sistema) use valores diferentes para *`etapa`* para indicar qual etapa da atualização você está registrando. Não ponha o arquivo de transcrição em um diretório temporário como `/tmp` ou `/var/tmp` (arquivos nesses diretórios podem ser excluídos durante a atualização ou durante qualquer reinicialização).

A transcrição também permitirá que você reveja informações que rolaram para fora da tela. Caso você esteja no console do sistema, apenas mude para VT2 (usando Alt + F2) e, após se autenticar, use `less -R ~root/upgrade-bullseye-etapa.script` para ver o arquivo.

Depois que você tiver completado a atualização, pode parar o **script** digitando `exit` no prompt.

O **apt** também regitrará os estados dos pacotes modificados em `/var/log/apt/history.log` e a saída do terminal em `/var/log/apt/term.log`. O **dpkg** registrará, adicionalmente, todas as modificações de estados de pacotes em `/var/log/dpkg.log`. Caso você use o **aptitude**, ele também registrará as modificações de estado em `/var/log/aptitude`.

Caso você tenha usado a opção *-t* para o **script**, você pode usar o programa **scriptreplay** para reproduzir toda a sessão:

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

4.4.2 Atualizando a lista de pacotes

Primeiro, a lista de pacotes disponíveis para a nova versão precisa ser obtida. Isso é feito executando:

```
# apt update
```

NOTA

Os usuários do apt-secure podem encontrar problemas ao usar **aptitude** ou **apt-get**. Para o apt-get, você pode usar **apt-get update --allow-releaseinfo-change**.

4.4.3 Certifique-se que você tem espaço suficiente para a atualização

Você tem que se certificar, antes de atualizar o seu sistema, que você terá espaço em disco rígido suficiente quando iniciar a atualização completa do sistema descrita em Seção 4.4.5. Primeiro, qualquer pacote necessário para instalação que for obtido pela rede é armazenado em `/var/cache/apt/archives` (e no subdiretório `partial/`, durante o download), então você deve certificar-se que tem espaço suficiente na partição do sistema de arquivos que contém o `/var/` para download temporário dos pacotes que serão instalados em seu sistema. Após o download, você provavelmente precisará de mais espaço em outras partições de sistemas de arquivos, tanto para instalação de pacotes atualizados (que podem conter executáveis maiores ou mais dados) quanto para novos pacotes que serão trazidos pela atualização. Caso o seu sistema não tenha espaço suficiente, você pode acabar com uma atualização incompleta que pode ser difícil de recuperar.

O **apt** pode exibir informações detalhadas sobre o espaço em disco necessário para a instalação. Antes de executar a atualização, você pode ver essa estimativa executando:

```
# apt -o APT::Get::Trivial-Only=true full-upgrade
[ ... ]
XXX atualizados, XXX novos instalados, XXX a remover e XXX não atualizados.
Necessário obter xx.xMB de arquivos.
Após essa operação, AAAMB de espaço de disco adicional serão usados.
```

NOTA

Ao executar esse comando no início do processo de atualização, pode ocorrer um erro, devido às razões descritas nas próximas seções. Nesse caso, você precisará esperar até que tenha feito a atualização mínima do sistema, como em Seção 4.4.4, antes de executar esse comando para estimar o espaço em disco.

Caso você não tenha espaço suficiente em disco para a atualização, o **apt** o avisará com uma mensagem como esta:

```
E: Você não tem espaço livre suficiente em /var/cache/apt/archives/.
```

Nessa situação, certifique-se de liberar espaço suficiente antes. Você pode:

- Remover pacotes que tenham sido previamente baixados para instalação (em `/var/cache/apt/archives`). Limpar o cache de pacotes executando **apt clean** removerá todos os arquivos de pacote previamente baixados.
- Remover pacotes esquecidos. Caso você tenha utilizado o **aptitude** ou **apt** para instalar pacotes manualmente na buster, ele terá mantido o registro desses pacotes que você instalou manualmente e será capaz de marcar como redundantes aqueles pacotes obtidos apenas por dependências que não são mais necessárias devido ao pacote ter sido removido. Eles não marcarão para remoção

pacotes que você instalou manualmente. Para remover automaticamente pacotes que não são mais usados, execute:

```
# apt autoremove
```

Você também pode usar o **deborphan**, **debfoster** ou **cruft** para encontrar pacotes redundantes. Não remova cegamente os pacotes apresentados por essas ferramentas, especialmente se você estiver usando opções agressivas diferentes do padrão que são propensas a falsos positivos. É altamente recomendado que você revise manualmente os pacotes sugeridos para remoção (ou seja, seus conteúdos, tamanhos e descrições) antes de removê-los.

- Remova pacotes que ocupam muito espaço e não são necessários atualmente (você sempre pode reinstalá-los após a atualização). Caso você tenha o `popularity-contest` instalado, você pode usar o **popcon-largest-unused** para listar os pacotes que você não usa e que ocupam mais espaço. Você pode encontrar apenas os pacotes que ocupam mais espaço em disco com **dpigs** (disponível no pacote `debian-goodies`) ou com o **wajig** (executando `wajig size`). Eles também podem ser encontrados com o `aptitude`. Inicie o **aptitude** em modo terminal cheio, selecione Visões → Nova lista de pacotes plana, pressione **l** e digite `~i`, então pressione **S** e digite `~installsize`. Isso lhe dará uma lista conveniente para trabalhar.
- Remover traduções e arquivos de localização do sistema se eles não forem necessários. Você pode instalar o pacote `localepurge` e configurá-lo para que apenas alguns locales selecionados sejam mantidos no sistema. Isso reduzirá o espaço de disco consumido em `/usr/share/locale`.
- Mover temporariamente para um outro sistema, ou remover permanentemente, registros do sistema existentes em `/var/log/`.
- Usar um `/var/cache/apt/archives` temporário: Você pode usar um diretório de cache temporário de um outro sistema de arquivos (dispositivo de armazenamento USB, disco rígido temporário, sistema de arquivos já em uso, ...).

NOTA

Não use uma montagem NFS pois a conexão de rede pode ser interrompida durante a atualização.

Por exemplo, caso você tenha um pendrive USB montado em `/media/pendrive`:

1. remova os pacotes que tenham sido previamente baixados para instalação:

```
# apt clean
```

2. copie o diretório `/var/cache/apt/archives` para o drive USB:

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

3. monte o diretório de cache temporário no lugar do atual:

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

4. após a atualização, restaure o diretório `/var/cache/apt/archives` original:

```
# umount /media/pendrive/archives
```

5. remova o `/media/pendrive/archives` restante.

Você pode criar o diretório de cache temporário em qualquer sistema de arquivos que esteja montado em seu sistema.

- Fazer uma atualização mínima do sistema (veja Seção 4.4.4) ou atualizações parciais do sistema seguidas por uma atualização completa. Isso permitirá atualizar o sistema parcialmente, e permite limpar o cache de pacotes antes da atualização completa.

Note que para remover pacotes com segurança, é aconselhável mudar os seus arquivos source-list do APT de volta para buster como descrito em Seção A.2.

4.4.4 Atualização mínima do sistema

IMPORTANTE

Se você estiver atualizando remotamente, esteja ciente da Seção 5.1.22.

Em alguns casos, fazer a atualização completa (como descrito abaixo) diretamente pode remover um grande número de pacotes que você queira manter. Nós portanto recomendamos um processo de atualização em duas partes: primeiro uma atualização mínima para superar esses conflitos, depois uma atualização completa como descrito em Seção 4.4.5.

Para fazer isso, primeiro execute:

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

Isso tem como efeito a atualização daqueles pacotes que podem ser atualizados sem a necessidade de que quaisquer outros pacotes sejam removidos ou instalados.

A atualização mínima do sistema também pode ser útil quando o sistema estiver com pouco espaço e uma atualização completa não puder ser feita devido às restrições de espaço.

Se o pacote `apt-listchanges` estiver instalado, ele mostrará (em sua configuração padrão) informações importantes sobre pacotes atualizados em um paginador depois de baixar os pacotes. Pressione **q** após a leitura para sair do paginador e continue a atualização.

4.4.5 Atualizando o sistema

Uma vez que você tenha cumprido os passos anteriores, agora está pronto para continuar com a parte principal da atualização. Execute:

```
# apt full-upgrade
```

Isso realizará uma atualização completa do sistema, instalando as versões mais novas disponíveis de todos os pacotes, e resolvendo todas as mudanças de dependências possíveis entre pacotes em lançamentos diferentes. Se necessário, instalará alguns pacotes novos (normalmente novas versões de bibliotecas, ou pacotes renomeados), e removerá quaisquer pacotes obsoletos em conflito.

Quando atualizar a partir de um conjunto de CDs/DVDs/BDs, será pedido para inserir discos específicos em vários pontos durante a atualização. Você pode ter que inserir o mesmo disco várias vezes; isso é devido a pacotes inter-relacionados que foram espalhados através dos discos.

As novas versões dos pacotes instalados atualmente que não puderem ser atualizadas sem mudar a situação da instalação de um outro pacote serão deixadas em sua versão atual (exibidas como "held back"). Isso pode ser resolvido tanto utilizando o **aptitude** para escolher esses pacotes para instalação, como tentando `apt install` *`pacote`*.

4.5 Possíveis problemas durante a atualização

As seções seguintes descrevem problemas conhecidos que podem aparecer durante uma atualização para a bullseye.

4.5.1 O dist-upgrade falha com "Could not perform immediate configuration"

Em alguns casos a etapa **apt full-upgrade** pode falhar após baixar os pacotes com:

```
E: Não foi possível realizar a configuração imediata no 'pacote'. Por favor, veja ↩
    man 5 apt.conf sob APT::Immediate-Configure para detalhes.
```

Caso isso ocorra, executar **apt full-upgrade -o APT::Immediate-Configure = 0** em vez disso deve permitir que a atualização prossiga.

Outra possível solução para esse problema é adicionar temporariamente as fontes do buster e bullseye aos seus arquivos source-list do APT e executar **apt update**.

4.5.2 Remoções esperadas

O processo de atualização para a bullseye pode solicitar a remoção de pacotes no sistema. A lista exata dos pacotes variará dependendo do conjunto de pacotes que você tenha instalado. Estas notas de lançamento dão conselhos gerais sobre essas remoções, mas se estiver em dúvida, é recomendado que você examine as remoções de pacotes propostas por cada método antes de prosseguir. Para mais informações sobre pacotes obsoletos no bullseye, veja Seção 4.8.

4.5.3 Loops de conflitos ou pré-dependências

Algumas vezes é necessário habilitar a opção `APT::Force-LoopBreak` no APT para que seja possível remover temporariamente um pacote essencial devido a um loop de "Conflitos/Pré-Dependências". O **apt** o alertará sobre isso e cancelará a atualização. Você pode contornar isso especificando a opção `-o APT::Force-LoopBreak=1` na linha de comando do **apt**.

É possível que uma estrutura de dependências do sistema possa estar tão corrompida de modo que necessite de intervenção manual. Normalmente, isso significa usar o **apt** ou

```
# dpkg --remove nome_do_pacote
```

para eliminar alguns dos pacotes problemáticos, ou

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

Em casos extremos, você poderá ter que forçar a reinstalação com um comando como

```
# dpkg --install /caminho/para/nome_do_pacote.deb
```

4.5.4 Conflitos de arquivo

Os conflitos de arquivo não devem ocorrer caso você atualize a partir de um sistema "puro" buster, mas podem ocorrer caso você tenha portes retroativos não oficiais instalados. Um conflito de arquivo resultará em um erro como:

```
Descompactando <pacote-foo> (de <arquivo-de-pacote-foo>) ...
dpkg: erro processando <pacote-foo> (--install):
 tentando sobrescrever '<algum-nome-de-arquivo>',
 que também está no pacote <pacote-bar>
dpkg-deb: sub-processo de colagem morto pelo sinal (pipe quebrado)
 Erros foram encontrados enquanto processando:
 <pacote-foo>
```

Você pode tentar resolver um conflito de arquivo com a remoção forçada do pacote mencionado na *última* linha da mensagem de erro:

```
# dpkg -r --force-depends nome_do_pacote
```

Após consertar as coisas, você deve ser capaz de continuar a atualização repetindo os comandos do **apt** descritos anteriormente.

4.5.5 Mudanças de configuração

Durante a atualização, serão feitas perguntas com relação a configuração ou reconfiguração de diversos pacotes. Quando você for perguntado se algum arquivo no diretório `/etc/init.d`, ou o arquivo `/etc/manpath.config` deve ser substituído pela versão do mantenedor do pacote, normalmente é necessário responder "yes" para garantir a coerência do sistema. Você sempre pode reverter para as versões antigas, já que serão guardadas com uma extensão `.dpkg-old`.

Caso você não tenha certeza do que fazer, anote o nome do pacote ou arquivo e resolva em um momento posterior. Você pode procurar no arquivo transcrito para rever as informações que estavam na tela durante a atualização.

4.5.6 Mudança de sessão para o console

Caso você esteja executando a atualização usando o console local do sistema, você pode achar que em alguns momentos durante a atualização o console é comutado para uma visão diferente e você perde a visibilidade do processo de atualização. Por exemplo, isso pode acontecer em sistemas com interface gráfica quando o gerenciador de tela é reiniciado.

Para recuperar o console onde a atualização estava em execução você terá que usar Ctrl + Alt + F1 (se estiver na tela de inicialização gráfica) ou Alt + F1 (se estiver no console local em modo texto) para mudar de volta para o terminal virtual 1. Substitua F1 pela tecla de função com o mesmo número do terminal virtual onde a atualização estava em execução. Você também pode usar Alt + Seta Esquerda ou Alt + Seta Direita para mudar entre os diferentes terminais em modo texto.

4.6 Atualizando o seu kernel e pacotes relacionados

Esta seção explica como atualizar o seu kernel e identifica potenciais problemas relacionados com essa atualização. Você pode instalar um dos pacotes `linux-image-*` fornecidos pelo Debian, ou compilar um kernel customizado a partir do fonte.

Note que muitas das informações nesta seção são baseadas na suposição de que você usará um dos kernels modulares do Debian, juntamente com o `initramfs-tools` e o `udev`. Caso você escolha utilizar um kernel customizado que não requeira uma initrd ou se você utilizar um gerador de initrd diferente, algumas das informações podem não ser relevantes para você.

4.6.1 Instalando um metapacote do kernel

Quando você fizer full-upgrade da buster para a bullseye, é fortemente recomendado que você instale um metapacote linux-image-*, caso você não tenha feito isso antes. Esses metapacotes trarão automaticamente uma nova versão do kernel durante as atualizações. Você pode verificar se você tem um instalado executando:

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

Caso você não veja nenhuma saída, então você precisará instalar um novo pacote linux-image manualmente ou instalar um metapacote linux-image. Para ver uma lista dos metapacotes linux-image disponíveis, execute:

```
# apt-cache search linux-image- | grep -i meta | grep -v transition
```

Caso você esteja inseguro sobre qual pacote selecionar, execute `uname -r` e procure um pacote com um nome semelhante. Por exemplo, caso você veja "`4.9.0.8-amd64`", é recomendado que você instale `linux-image-amd64`. Você também pode usar **apt** para ver uma descrição longa de cada pacote a fim de ajudar a escolher o melhor disponível. Por exemplo:

```
# apt show linux-image-amd64
```

Você deve então usar `apt install` para instalá-lo. Uma vez que o novo kernel esteja instalado, você deverá reinicializar assim que for possível para obter os benefícios oferecidos pela nova versão do kernel. Porém, por favor, consulte Seção 5.1.24 antes de realizar a primeira reinicialização após a atualização.

Para os mais aventureiros, existe uma forma fácil de compilar seu próprio kernel customizado no Debian. Instale os fontes do kernel, fornecidos no pacote `linux-source`. Você pode fazer uso do alvo `deb-pkg` disponível no makefile dos fontes para construir um pacote binário. Mais informações podem ser encontradas no Debian Linux Kernel Handbook (`https://kernel-team.pages.debian.net/kernel-handbook/`), o qual também pode ser encontrado como o pacote `debian-kernel-handbook`.

Se possível, é vantajoso atualizar o pacote do kernel separadamente do `full-upgrade` principal para reduzir as chances de ter um sistema temporariamente não inicializável. Note que isso deve ser feito somente após o processo de atualização mínima descrito em Seção 4.4.4.

4.7 Preparar para a próxima versão

Após a atualização, existem diversas coisas que você pode fazer para preparar para a próxima versão.

- Remova pacotes redundantes recentemente ou obsoletos como descrito em Seção 4.4.3 e Seção 4.8. Você deve rever quais arquivos de configuração eles usam e considerar expurgar os pacotes para remover seus arquivos de configuração. Veja também Seção 4.7.1.

4.7.1 Expurgando pacotes removidos

Em geral, é aconselhável expurgar pacotes removidos. Isso é especialmente verdadeiro caso os mesmos tenham sido removidos em uma atualização da versão anterior (por exemplo, de uma atualização do buster) ou foram fornecidos por terceiros. Em particular, scripts antigos init.d têm sido conhecidos por causarem problemas.

> **CUIDADO**
>
> Ao expurgar um pacote, geralmente os seus arquivos de log também serão expurgados, então, é possível que você queira fazer um backup deles primeiro.

O seguinte comando apresenta uma lista de todos os pacotes removidos que podem ter deixado arquivos de configuração no sistema (se houver):

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

Os pacotes podem ser removidos utilizando **apt purge**. Supondo que você queira expurgar todos eles de uma vez, você pode usar o seguinte comando:

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

Caso você utilize o `aptitude`, você também pode usar a seguinte alternativa para os comandos acima:

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

4.8 Pacotes obsoletos

Ao introduzir vários novos pacotes, a bullseye também aposenta e omite muitos pacotes antigos que estavam na buster. Não é fornecido um caminho de atualização para esses pacotes obsoletos. Apesar de nada lhe impedir de continuar a usar um pacote obsoleto enquanto o desejar, o projeto Debian normalmente descontinuará o suporte de segurança para o mesmo um ano após o lançamento da bullseye[5], e não fornecerá normalmente outro suporte nesse meio tempo. Substituí-los por alternativas disponíveis, caso existam, é recomendado.

Existem muitas razões pela quais os pacotes podem ter sido removidos da distribuição: eles não são mais mantidos pelo upstream; não existe mais nenhum Desenvolvedor Debian interessado em manter os pacotes; a funcionalidade que eles fornecem foi substituída por um software diferente (ou uma nova versão); ou eles não são mais considerados adequados para o bullseye devido a bugs nos mesmos. Nesse último caso, os pacotes podem ainda estar presentes na distribuição "unstable".

Algumas interfaces de gerenciamento de pacotes fornecem maneiras fáceis de encontrar pacotes instalados que não estão mais disponíveis a partir de quaisquer repositórios conhecidos. A interface de usuário textual do **aptitude** os lista na categoria "Pacotes obsoletos e criados localmente", e eles podem ser listados e expurgados a partir da linha de comando com:

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

O Sistema de Rastreamento de Bugs do Debian (`https://bugs.debian.org/`) frequentemente fornece informações adicionais sobre a razão da remoção do pacote. Você deve revisar tanto os relatórios de bug arquivados para o próprio pacote quanto os relatórios de bug arquivados para o pseudo-pacote ftp.debian.org (`https://bugs.debian.org/cgi-bin/pkgreport.cgi?pkg=ftp.debian.org&archive=yes`).

Para uma lista de pacotes obsoletos para a Bullseye, por favor, consulte Seção 5.3.1.

4.8.1 Pacotes fictícios transitórios

Alguns pacotes da buster podem ter sido substituídos na bullseye por pacotes fictícios transitórios, os quais são substitutos projetados para simplificar as atualizações. Se, por exemplo, um aplicativo que anteriormente era um pacote simples foi dividido em vários pacotes, um pacote transitório pode ser fornecido com o mesmo nome do pacote antigo e com dependências apropriadas para fazer com que os novos pacotes sejam instalados. Depois disso ter acontecido, o pacote fictício redundante pode ser removido seguramente.

As descrições dos pacotes fictícios transitórios geralmente indicam o seu propósito. No entanto, elas não são uniformes; em particular, alguns pacotes fictícios ("dummy") são projetados para continuarem instalados, com a finalidade de incluir uma suíte de software completa, ou acompanhar a última versão atual de algum programa. Você pode também considerar útil o **deborphan** com as opções `--guess-*` (por exemplo, `--guess-dummy`) para detectar pacotes fictícios transitórios em seu sistema.

[5] Ou enquanto não existir outro lançamento durante esse período de tempo. Normalmente, apenas duas versões estáveis são suportadas em um dado momento.

Capítulo 5

Problemas a serem considerados para a bullseye

Algumas vezes, mudanças introduzidas em uma nova versão têm efeitos colaterais que não podem ser evitados ou que acabam expondo bugs em outros locais. Esta seção documenta problemas conhecidos. Por favor, leia também a errata, a documentação dos pacotes relevantes, relatórios de bugs e outras informações mencionadas em Seção 6.1.

5.1 Itens específicos da atualização para bullseye

Esta seção aborda itens relacionados à atualização da buster para a bullseye.

5.1.1 O sistema de arquivos XFS não suporta mais a opção barrier/nobarrier

O suporte às opções de montagem `barrier` e `nobarrier` foi removido do sistema de arquivos XFS. É recomendado checar `/etc/fstab` pela presença de uma dessas palavras e removê-la. Partições usando essas opções vão falhar ao montar.

5.1.2 Disposição do repositório de seguraça alterada

Para a bullseye, a suíte de segurança é agora chamada `bullseye-security` em vez de *`codinome`*`/updates`, e usuários devem adaptar seus arquivos source-list do APT adequadamente ao atualizar.

A linha de segurança em sua configuração do APT pode parecer com:

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

Se a sua configuração do APT também envolve "pinning" ou `APT::Default-Release`, provavelmente serão necessários ajustes, uma vez que o codinome do repositório de segurança não combina mais com o codinome do repositório regular. Um exemplo de uma linha `APT::Default-Release` funcional para a bullseye se parece com:

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

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

5.1.3 Hash de senha usa yescrypt por padrão

O hash de senha padrão para contas de sistema locais foi alterado (`https://tracker.debian.org/news/1226655/accepted-pam-140-3-source-into-unstable/`) de SHA-512 para yescrypt (`https://www.openwall.com/yescrypt/`) (veja crypt(5) (`https://manpages.debian.org//bullseye/libcrypt-dev/crypt.5.html`)). É esperado que isso ofereça maior segurança com relação a ataques de adivinhação de senha baseado em dicionário, em termos da complexidade tanto de espaço quanto de tempo do ataque.

Para tirar proveito desta melhoria em segurança, altere senhas locais; por exemplo, use o comando **passwd**.

Senhas antigas continuarão funcionando usando qualquer que seja o hash de senha usado para criá-las.

Yescrypt não é suportado por Debian 10 (buster). Consequentemente, arquivos de senha shadow (`/etc/shadow`) não podem ser copiados de um sistema bullseye de volta para um sistema buster. Se esses arquivos forem copiados, senhas que foram alteradas no sistema bullseye não funcionarão no sistema buster. Similarmente, hashes de senha não podem ser copiados&colados de um sistema bullseye para buster.

Se for necessário compatibilidade para hashes de senha entre bullseye and buster, modifique `/etc/pam.d/common-password`. Encontre a linha que se parece com:

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

e substitua `yescrypt` por `sha512`.

5.1.4 Suporte a NSS NIS e NIS+ exige novos pacotes

O suporte a NSS NIS e NIS+ foi movido para pacotes separados, chamados `libnss-nis` e `libnss-nisplus`. Infelizmente, `glibc` não pode depender desses pacotes e, por esse motivo, eles são somente recomendados agora.

Em sistemas usando NIS ou NIS+, portanto, é recomendado conferir se esses pacotes estão instalados corretamente depois da atualização.

5.1.5 Gerenciamento de fragmentos de arquivos de configuração no "unbound"

O resolvedor DNS `unbound` mudou a forma de gerenciar fragmentos de arquivos de configuração. Se você está usando uma diretiva `include:` para unir vários fragmentos em uma única configuração válida, você deveria ler o arquivo NEWS (`https://sources.debian.org/src/unbound/bullseye/debian/NEWS/`).

5.1.6 Obsolescência de parâmetros do rsync

Os parâmetros `--copy-devices` e `--noatime` do `rsync` foram renomeados para `--write-devices` e `--open-noatime`. As formas antigas não têm mais suporte; se você as está usando, você deve ler o arquivo NEWS (`https://sources.debian.org/src/rsync/bullseye/debian/rsync.NEWS/`). Processos de transferência entre sistemas executando versões diferentes do Debian podem exigir que a parte com buster seja atualizada para uma versão do `rsync` do repositório backports (`https://backports.debian.org/`).

5.1.7 Gerenciamento de "addons" do Vim

Os "addons" para o `vim`, historicamente fornecidos por `vim-scripts`, agora são gerenciados pela funcionalidade "package" nativa do Vim, em vez de pelo `vim-addon-manager`. Usuários do Vim devem agir antes da atualização, seguindo as instruções do arquivo NEWS (`https://sources.debian.org/src/vim-scripts/bullseye/debian/NEWS/`).

5.1.8 OpenStack e cgroups v1

O OpenStack Victoria (lançado na bullseye) exige cgroup v1 para QoS de dispositivos de bloco. Uma vez que a bullseye também mudou para o uso de cgroupv2 por padrão (veja Seção 2.2.4), a árvore sysfs em `/sys/fs/cgroup` não incluirá funcionalidades cgroup v1 tais como `/sys/fs/cgroup/blkio` e, como resultado, **cgcreate -g blkio:foo** falhará. Para nós OpenStack executando `nova-compute` ou `cinder-volume`, é fortemente aconselhado adicionar os parâmetros `systemd.unified_cgroup_hierarchy=false` e `systemd.legacy_systemd_cgroup_controller=false` à linha de comando do kernel, para sobrepor o padrão e restaurar a antiga hierarquia cgroup.

5.1.9 Arquivos de política da API do OpenStack

Seguindo as recomendações do autor original, o OpenStack Victoria, na versão distribuída na bullseye, passa a usar o novo formato YAML para a API do OpenStack. Como resultado, a maioria dos serviços OpenStack, incluindo Nova, Glance e Keystone, aparecem quebrados, com todas as políticas da API escritas explicitamente em arquivos `policy.json`. Portanto, pacotes agora vêm com um diretório `/etc/PROJECT/policy.d` contendo um arquivo `00_default_policy.yaml`, com todas as políticas comentadas por padrão.

Para evitar que o antigo arquivo `policy.json` continue ativo, os pacotes Debian do OpenStack agora renomeiam tal arquivo como `disabled.policy.json.old`. Em alguns casos, quando nenhuma alternativa melhor pôde ser implementada em tempo hábil para o lançamento, o arquivo `policy.json` é, até mesmo, simplesmente deletado. Portanto, antes da atualização, é fortemente aconselhado fazer cópias de segurança dos arquivos `policy.json` das suas instalações.

Mais detalhes estão disponíveis na documentação do autor original (`https://governance.openstack.org/tc/goals/selected/wallaby/migrate-policy-format-from-json-to-yaml.html`).

5.1.10 Indisponibilidade do sendmail durante a atualização

Em contraste com as atualizações normais do `sendmail`, durante a atualização da buster para a bullseye o serviço sendmail será parado, causando mais indisponibilidade que o usual. Para aconselhamento genérico sobre redução de indisponibilidade, veja Seção 4.1.3.

5.1.11 FUSE 3

Alguns pacotes, incluindo `gvfs-fuse`, `kio-fuse` e `sshfs`, mudaram para FUSE 3. Durante as atualizações, isso fará com que `fuse3` seja instalado e `fuse` seja removido.

Em algumas circunstâncias excepcionais, por exemplo, ao fazer a atualização somente executando **apt-get dist-upgrade** em vez de seguir os passos de atualização recomendados em Capítulo 4, os pacotes que dependem de `fuse3` podem ser mantidos nas suas versões antigas durante a atualização. Executar os passos discutidos em Seção 4.4.5 novamente com o `apt` da bullseye, ou atualizá-los manualmente, resolverá a situação.

5.1.12 Arquivo de opções do GnuPG

A partir da versão 2.2.27-1, a configuração por usuário da suíte `GnuPG` foi completamente movida para `~/.gnupg/gpg.conf`, e `~/.gnupg/options` não é mais utilizado. Por favor, renomeie o arquivo se necessário, ou mova o seu conteúdo para o novo local.

5.1.13 Linux habilita espaços de nomes por padrão

A partir do `Linux` 5.10, todos os usuários têm permissão para criar espaços de nomes ("namespaces") de usuário por padrão. Isso permitirá que programas, tais como navegadores web e gerenciadores de contêineres, criem caixas de areia ("sandboxes") mais restritas para código não confiável ou menos confiável, sem a necessidade de executar como root ou usar um comando auxiliar setuid-root.

O padrão anterior adotado pelo Debian era restringir essa funcionalidade a processos executando como root, porque isso expunha mais problemas de segurança no kernel. No entanto, como a implementação dessa funcionalidade amadureceu, nós agora estamos seguros de que os benefícios de segurança fornecidos por ela são muito maiores do que o risco de habilitá-la.

Se você prefere manter essa funcionalidade restrita, defina o sysctl:

```
user.max_user_namespaces = 0
```

Note que várias funcionalidades de ambientes de área de trabalho e de contêineres não funcionarão com essa restrição ativa, incluindo navegadores web, `WebKitGTK`, `Flatpak` e geração de miniaturas de imagens ("thumbnailing") no `GNOME`.

O sysctl específico do Debian `kernel.unprivileged_userns_clone=0` tem um efeito similar, mas está obsoleto.

5.1.14 Linux desabilita chamadas não privilegiadas a bpf() por padrão

A partir do `Linux` 5.10, o Debian desabilita chamadas não privilegiadas a bpf() por padrão. No entanto, um administrador ainda pode mudar essa configuração posteriormente, se necessário, escrevendo 0 ou 1 no sysctl `kernel.unprivileged_bpf_disabled`.

Se você prefere manter chamadas não privilegiadas a bpf() habilitadas, defina o sysctl:

```
kernel.unprivileged_bpf_disabled = 0
```

Para mais informação sobre a mudança como padrão no Debian, veja o bug 990411 (`https://bugs.debian.org/990411`) para a solicitação da mudança.

5.1.15 Redmine faltando na bullseye

O pacote `redmine` não é fornecido na bullseye, pois se tornou muito tarde para migrar da antiga versão do `rails`, o qual está no final do suporte do autor original (recebendo somente correções para bugs de segurança severos) para a versão que está na bullseye. Os mantenedores de `Ruby Extras` estão acompanhando de perto os autores originais e liberarão uma versão via backports (`https://backports.debian.org/`) tão logo quanto ela seja disponibilizada e eles tenham pacotes em funcionamento. Se você não pode aguardar para que isso aconteça antes de atualizar, você pode usar uma máquina virtual ou contêiner executando buster para isolar essa aplicação específica.

5.1.16 Exim 4.94

Por favor, considere que a versão do Exim na bullseye é uma *grande* atualização do Exim. Ela introduz o conceito de dados contaminados ("tainted"), lidos a partir de fontes não confiáveis, como, por exemplo, o remetente ou o destinatário da mensagem. Esses dados contaminados (p.ex. `$local_part` ou `$domain`) não podem ser usados, entre outras coisas, como nomes de arquivos ou diretórios, ou nomes de comandos.

Isso *quebrará* configurações que não sejam atualizadas de acordo. Antigos arquivos do Debian de configuração do Exim também não funcionarão sem modificação. A nova configuração precisa ser instalada preservando as modificações locais, unindo-as.

Exemplos típicos que não funcionam incluem:

- Entrega para `/var/mail/$local_part`. Use `$local_part_data` em combinação com `check_local_user`.
- Usar

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

  em vez de

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

  para um arquivo de "alias" de domínio virtual.

A estratégia básica para lidar com essa mudança é usar o resultado de uma consulta ("lookup") em processamentos adicionais em vez de usar o resultado original (obtido remotamente).

Para facilitar a atualização, existe uma nova opção de configuração principal para temporariamente rebaixar erros de contaminação ("taint") para avisos, deixando a antiga configuração funcionar com a nova versão do Exim. Para usar essa funcionalidade, adicione

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

à configuração do Exim (p.ex. em `/etc/exim4/exim4.conf.localmacros`) *antes* de atualizar, e verifique o arquivo de log pela presença de avisos de contaminação ("taint"). Essa é uma medida paliativa temporária, que já está marcada para remoção desde a sua introdução.

5.1.17 Sondagem de dispositivos SCSI é não determinística

Devido a mudanças no kernel Linux, a sondagem de dispositivos SCSI deixou de ser determinística. Isso pode ser um problema para instalações que dependem da ordem de sondagem dos discos. Duas possíveis alternativas usando links em `/dev/disk/by-path` ou uma regra `udev` são sugeridas nesta postagem em lista de e-mails (`https://lore.kernel.org/lkml/59eedd28-25d4-7899-7c3c-89fe7fdd4b43@acm.org/`).

5.1.18 rdiff-backup requer atualização sincronizada do servidor e cliente

Os protocolos de rede das versões 1 e 2 do `rdiff-backup` são incompatíveis. Isso significa que você deve executar a mesma versão (ou 1 ou 2) do `rdiff-backup` localmente e remotamente. Uma vez que a buster distribui a versão 1.2.8 e a bullseye distribui a versão 2.0.5, atualizar somente o sistema local ou somente o sistema remoto da buster para a bullseye quebrará as execuções do `rdiff-backup` entre os dois.

A versão 2.0.5 do `rdiff-backup` está disponível no repositório buster-backports, veja backports (`https://backports.debian.org/`). Isso permite aos usuários atualizarem primeiro somente o pacote `rdiff-backup` nos seus sistemas buster, e depois atualizar independentemente os sistemas para a bullseye quando for conveniente.

5.1.19 Problemas com microcódigo para CPU Intel

O pacote `intel-microcode` atualmente na bullseye e buster-security (veja DSA-4934-1 (`https://www.debian.org/security/2021/dsa-4934`)) contém sabidamente dois bugs significantes. Para algumas CPUs CoffeeLake, esta atualização pode quebrar interfaces de rede (`https://github.com/intel/Intel-Linux-Processor-Microcode-Data-Files/issues/56`) que usam `firmware-iwlwifi`, e para algumas CPUs Skylake R0/D0 em sistemas usando um firmware/BIOS muito desatualizado, o sistema pode travar na inicialização (`https://github.com/intel/Intel-Linux-Processor-Microcode-Dat issues/31`).

Se você não fez a atualização do DSA-4934-1 devido a algum desses problemas, ou não tem o repositório de segurança habilitado, esteja ciente de que atualizar para o pacote `intel-microcode` na bullseye pode causar o travamento do seu sistema ao inicializar, ou quebrar o iwlwifi. Nesse caso, você pode recuperar desabilitando o carregamento do microcódigo na inicialização; veja as instruções no DSA, as quais também estão no `README.Debian` do `intel-microcode`.

5.1.20 Atualizações envolvendo libgc1c2 precisam de duas execuções

Pacotes que dependem de `libgc1c2` na buster (p.ex. `guile-2.2-libs`) podem ser retidos durante a primeira execução da atualização completa para a bullseye. Fazer uma segunda atualização, normalmente, resolve o problema. As informações sobre o problema podem ser encontradas no bug #988963 (`https://bugs.debian.org/988963`).

5.1.21 fail2ban não consegue enviar e-mail usando mail de bsd-mailx

O pacote `fail2ban` pode ser configurado para enviar notificações por e-mail. Ele faz isso usando **mail**, o qual é fornecido por múltiplos pacotes no Debian. Uma atualização de segurança (necessária em sistemas que usam **mail** do `mailutils`) pouco antes do lançamento da bullseye quebrou essa funcionalidade para sistemas que têm **mail** fornecido por `bsd-mailx`. Usuários do `fail2ban` em combinação com `bsd-mailx` que desejarem que o `fail2ban` envie e-mail devem ou trocar para um fornecedor diferente para **mail** ou manualmente desaplicar o commit do fornecedor original (`https://github.com/fail2ban/fail2ban/commit/410a6ce5c80dd981c22752da034f2529b5eee844`) (que inseriu a sequência "`-E 'set escape'`" em múltiplos locais sob `/etc/fail2ban/action.d/`).

5.1.22 Novas conexões SSH não são possíveis durante a atualização

Apesar de que conexões Secure Shell (SSH) existentes devam continuar funcionando durante a atualização como usual, devido a circunstâncias infelizes, o período enquanto novas conexões SSH não podem ser estabelecidas é maior que o usual. Se a atualização está sendo feita sobre uma conexão SSH que pode ser interrompida, é recomendado atualizar o `openssh-server` antes de atualizar o sistema completo.

5.1.23 Open vSwitch upgrade requires interfaces(5) change

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

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

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

5.1.24 Coisas para fazer depois da atualização e antes de reinicializar

Quando o `apt full-upgrade` terminar, a atualização "formal" estará completa. Para a atualização da bullseye, não é necessária nenhuma ação especial antes de executar uma reinicialização.

5.2 Itens não limitados ao processo de atualização

5.2.1 Limitações no suporte de segurança

Há alguns pacotes onde o Debian não pode prometer fornecer portes retroativos mínimos para problemas de segurança. Esses são abordados nas subseções a seguir.

NOTA

O pacote `debian-security-support` ajuda a acompanhar a situação do suporte de segurança dos pacotes instalados.

5.2.1.1 Situação da segurança dos navegadores web e seus motores de renderização

O Debian 11 inclui diversos motores de navegadores que são afetados por um fluxo constante de vulnerabilidades de segurança. A alta taxa de vulnerabilidades e a ausência parcial de suporte do upstream na forma de ramos de longo prazo tornam muito difícil o suporte a esses navegadores e motores com correções de segurança portadas retroativamente. Além disso, as interdependências das bibliotecas tornam extremamente difícil atualizar para versões upstream mais novas. Por isso, navegadores feitos, por exemplo, sobre os motores webkit e khtml[1] foram incluídos na bullseye, mas não estão cobertos pelo suporte de segurança. Esses navegadores não devem ser usados em sites web não confiáveis. Os motores webkit2gtk e wpewebkit *são* cobertos pelo suporte de segurança.

Para o uso geral de um navegador web, nós recomendamos o Firefox ou o Chromium. Eles serão mantidos atualizados reconstruindo as versões ESR correntes para a stable. A mesma estratégia será aplicada para o Thunderbird.

5.2.1.2 OpenJDK 17

O Debian bullseye vem com uma versão de acesso antecipado do `OpenJDK 17` (a próxima versão esperada do `OpenJDK LTS` depois do `OpenJDK 11`), para evitar o tedioso processo de inicialização ("bootstrap"). O plano é que o `OpenJDK 17` receba uma atualização na bullseye para a versão final do autor original anunciada para outubro de 2021, seguida de atualizações de segurança em base de melhor esforço, mas os usuários não devem esperar ver atualizações para cada atualização de segurança trimestral do autor original.

[1] Esses motores são distribuídos em vários pacotes fonte diferentes e o problema se aplica a todos os pacotes que os distribuem. O problema também se estende a motores de renderização web não mencionados explicitamente aqui, com exceção de webkit2gtk e o novo wpewebkit.

5.2.1.3 Pacotes baseados em Go

Atualmente, a infraestrutura do Debian apresenta problemas para reconstruir pacotes de tipos que sistematicamente usam ligação estática. Antes da buster, isso não era um problema na prática, mas com o crescimento do ecossistema Go, isso significa que os pacotes baseados em Go serão cobertos por suporte de segurança limitado até que a infraestrutura seja aprimorada para lidar com eles de forma a facilitar a sua manutenção.

Se forem necessárias atualizações para bibliotecas de desenvolvimento Go, elas podem ser distribuídas somente através dos lançamentos pontuais regulares, o que pode demorar a acontecer.

5.2.2 Acessando o aplicativo Configurações do GNOME sem mouse

Sem um dispositivo apontador, não há um modo direto de alterar as configurações no aplicativo Configurações do GNOME fornecido por `gnome-control-center`. Para contornar isso, você pode navegar para o conteúdo principal a partir da barra lateral, pressionando **Seta Direita** duas vezes. Para voltar para a barra lateral, você pode iniciar uma pesquisa com Ctrl+F, digitar algo, e então teclar **Esc** para cancelar a pesquisa. Então, você pode usar **Seta para Cima** e **Seta para Baixo** para navegar pela barra lateral. Não é possível selecionar os resultados da pesquisa pelo teclado.

5.2.3 A opção de inicialização `rescue` não é utilizável sem uma senha de root

Com a implementação de `sulogin` usada desde a buster, inicializar com a opção `rescue` sempre requer a senha de root. Se uma senha de root não foi previamente definida, isso torna o modo de recuperação efetivamente não utilizável. No entanto, ainda é possível inicializar usando o parâmetro `init=/sbin/sulogin --force` do kernel.

Para configurar o systemd para fazer o equivalente a isso sempre que ele inicializar no modo de recuperação (também conhecido como modo "single": veja systemd(1) (`https://manpages.debian.org//bullseye/systemd/systemd.1.html`)), execute **sudo systemctl edit rescue.service** e crie um arquivo contendo somente isto:

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

Também (ou alternativamente) pode ser útil fazer isso para a "unit" `emergency.service`, a qual é iniciada *automaticamente* no caso de certos erros (veja systemd.special(7) (`https://manpages.debian.org//bullseye/systemd/systemd.special.7.html`)), ou se `emergency` for adicionado à linha de comando do kernel (p.ex. se o sistema não pode ser recuperado usando o modo de recuperação).

Para mais informação e uma discussão sobre as implicações de segurança, veja #802211 (`https://bugs.debian.org//802211`).

5.3 Obsolescência e depreciação

5.3.1 Pacotes obsoletos dignos de nota

A seguinte lista é de pacotes conhecidos e obsoletos dignos de nota (veja Seção 4.8 para uma descrição).

A lista de pacotes obsoletos inclui:

- O pacote `lilo` foi removido da bullseye. O sucessor do lilo como carregador de inicialização é o `grub2`.
- A versão 3 da suíte de gerenciamento de listas de e-mail Mailman é a única versão que está disponível neste lançamento. O Mailman foi dividido em vários componentes; o núcleo está disponível no pacote `mailman3` e a suíte completa pode ser obtida via o meta pacote `mailman3-full`.

  A versão legada 2.1 do Mailman não está mais disponível (costumava ser o pacote `mailman`). Essa versão depende do Python 2, que não está mais disponível no Debian.

  Para instruções de atualização, por favor, veja a documentação sobre migração do projeto. (`https://docs.mailman3.org/en/latest/migration.html`)

- O kernel Linux não fornece mais suporte a `isdn4linux` (i4l). Consequentemente, os pacotes de espaço de usuário `isdnutils`, `isdnactivecards`, `drdsl` e `ibod` foram removidos do repositório.

- As bibliotecas obsoletas libappindicator não são mais fornecidas. Como resultado, os pacotes relacionados `libappindicator1`, `libappindicator3-1` e `libappindicator-dev` não estão mais disponíveis. É esperado que isso cause erros de dependência para software de terceiros que ainda dependa de libappindicator para fornecer suporte a indicador e bandeja do sistema.

  O Debian está usando `libayatana-appindicator` como sucessor de libappindicator. Para informação técnica, veja este anúncio (`https://lists.debian.org/debian-devel/2018/03/msg00506.html`).

- O Debian não fornece mais o pacote `chef`. Se você usa Chef para gerenciamento de configuração, o melhor caminho de atualização provavelmente seja passar a usar o pacote fornecido por Chef Inc (`https://www.chef.io/`).

  Para informação sobre a remoção, veja a solicitação de remoção (`https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=963750`).

- O Python 2 já está além do final do seu ciclo de vida, e não receberá mais atualizações de segurança. Ele não tem suporte para a execução de aplicativos, e pacotes que dependem dele foram convertidos para Python3 ou foram removidos. No entanto, o Debian bullseye ainda inclui uma versão de Python 2.7, assim como uma pequena quantidade de ferramentas de desenvolvimento do Python 2, tais como `python-setuptools`. Elas estão presentes somente porque são necessárias para o processo de construção de alguns poucos aplicativos que ainda não foram convertidos para Python 3.

- O pacote `aufs-dkms` não faz parte da bullseye. A maioria dos usuários de `aufs-dkms` deve ser capaz de trocar para `overlayfs`, o qual fornece funcionalidade similar com suporte no kernel. No entanto, existe a possibilidade de ter uma instalação Debian em um sistema de arquivos que não seja compatível com `overlayfs`, p.ex. `xfs` sem `d_type`. Usuários do `aufs-dkms` são aconselhados a migrar do `aufs-dkms` antes de atualizar para a bullseye.

- O gerenciador de conexões de rede `wicd` não estará mais disponível depois da atualização. Para evitar o perigo de perder conectividade, é recomendado que os usuários troquem para uma alternativa como `network-manager` ou `connman` antes da atualização.

5.3.2 Componentes obsoletos para a bullseye

Com a próxima versão do Debian 12 (codinome bookworm), alguns recursos ficarão obsoletos. Os usuários precisarão migrar para outras alternativas para evitar problemas quando atualizarem para o Debian 12.

Isso inclui os seguintes recursos:

- As justificativas históricas para a disposição do sistema de arquivos com diretórios `/bin`, `/sbin` e `/lib` separados de seus equivalentes sob `/usr` não se aplicam mais atualmente; veja o resumo em Freedesktop.org (`https://www.freedesktop.org/wiki/Software/systemd/TheCaseForTheUsrMerge`). O Debian bullseye será a última versão do Debian com suporte à disposição "non-merged-usr". Para sistemas com uma disposição legada que foram atualizados sem uma reinstalação, existe o pacote `usrmerge` para fazer a conversão, caso desejado.

- A bullseye é a última versão do Debian a distribuir **apt-key**. Em vez disso, as chaves devem ser gerenciadas copiando arquivos em `/etc/apt/trusted.gpg.d`, em formato binário, tal como criado por **gpg --export**, com uma extensão `.gpg`, ou em formato ASCII, com uma extensão `.asc`.

  É planejado um substituto para **apt-key list** para investigar manualmente o chaveiro, mas o trabalho ainda não foi iniciado.

- Os "backends" de banco de dados do `slapd` slapd-bdb(5) (`https://manpages.debian.org//bullseye/slapd/slapd-bdb.5.html`), slapd-hdb(5) (`https://manpages.debian.org//bullseye/slapd/slapd-hdb.5.html`), e slapd-shell(5) (`https://manpages.debian.org//bullseye/slapd/slapd-shell.5.html`) estão sendo aposentados e não serão incluídos no

Debian 12. Bancos de dados LDAP usando os "backends" `bdb` ou `hdb` devem ser migrados para o "backend" slapd-mdb(5) (`https://manpages.debian.org//bullseye/slapd/slapd-mdb.5.html`).

Adicionalmente, os "backends" slapd-perl(5) (`https://manpages.debian.org//bullseye/slapd/slapd-perl.5.html`) e slapd-sql(5) (`https://manpages.debian.org//bullseye/slapd/slapd-sql.5.html`) estão obsoletos e podem ser removidos em um lançamento futuro.

O projeto OpenLDAP não tem suporte a "backends" aposentados ou obsoletos. Suporte para esses "backends" no Debian 11 é feito em uma base de melhor esforço.

5.4 Bugs severos conhecidos

Apesar de o Debian ser lançado quando está pronto, isso infelizmente não significa que não existam bugs conhecidos. Como parte do processo de lançamento, todos os bugs com severidade séria ou mais alta são ativamente acompanhados pela Equipe de Lançamento, assim uma visão geral desses bugs (`https://bugs.debian.org/cgi-bin/pkgreport.cgi?users=release.debian.org@packages.debian.org;tag=bullseye-can-defer`) que foram marcados para serem ignorados na última parte do lançamento da bullseye podem ser encontrados no Sistema de Acompanhamento de Bugs do Debian (`https://bugs.debian.org/`). Os seguintes bugs afetavam a bullseye no momento do lançamento e merecem menção neste documento:

Número do bug	Pacote (fonte ou binário)	Descrição
922981 (`https://bugs.debian.org/922981`)	`ca-certificates-java`	ca-certificates-java: /etc/ca-certificates/update.d/jks-keystore não atualiza /etc/ssl/certs/java/cacerts
990026 (`https://bugs.debian.org/990026`)	`cron`	cron: Conjunto de caracteres reduzido em MAILTO causa quebra
991081 (`https://bugs.debian.org/991081`)	`gir1.2-diodon-1.0`	gir1.2-diodon-1.0 tem falta de dependências
990318 (`https://bugs.debian.org/990318`)	`python-pkg-resources`	python-pkg-resources: favor adicionar "Breaks" contra os pacotes python não versionados
991449 (`https://bugs.debian.org/991449`)	`fail2ban`	correção para CVE-2021-32749 quebra sistemas com mail de bsd-mailx
990708 (`https://bugs.debian.org/990708`)	`mariadb-server-10.5,galera-4`	mariadb-server-10.5: problemas na atualização devidos à troca galera-3 -> galera-4
980429 (`https://bugs.debian.org/980429`)	`src:gcc-10`	g++-10: falha de segmentação espúria no modo c++17 em append_to_statement_list_1 (tree-iterator.c:65)
980609 (`https://bugs.debian.org/980609`)	`src:gcc-10`	falta i386-cpuinfo.h
984574 (`https://bugs.debian.org/984574`)	`gcc-10-base`	gcc-10-base: favor adicionar Breaks: gcc-8-base (<< 8.4)
984931 (`https://bugs.debian.org/984931`)	`git-el`	git-el,elpa-magit: falha ao instalar: /usr/lib/emacsen-common/packages/install/git emacs falhou em /usr/lib/emacsen-common/lib.pl linha 19, <TSORT> linha 7.
987264 (`https://bugs.debian.org/987264`)	`git-el`	git-el: falha ao instalar com xemacs21

Número do bug	Pacote (fonte ou binário)	Descrição
991082 (https://bugs.debian.org/991082)	gir1.2-gtd-1.0	gir1.2-gtd-1.0 tem "Depends" vazio
948739 (https://bugs.debian.org/948739)	gparted	gparted não deveria mascarar "units" .mount
984714 (https://bugs.debian.org/984714)	gparted	gparted deveria sugerir exfat-progs e fazer "backport" do "commit" que rejeita exfat-utils
968368 (https://bugs.debian.org/968368)	ifenslave	ifenslave: a opção bond-master falha ao adicionar interface ao "bond"
990428 (https://bugs.debian.org/990428)	ifenslave	ifenslave: "bonding" não funcionando na bullseye (usando configuração bond-slaves)
991113 (https://bugs.debian.org/991113)	libpam-chroot	libpam-chroot instala pam_chroot.so no diretório incorreto
989545 (https://bugs.debian.org/989545)	src:llvm-toolchain-11	libgl1-mesa-dri: si_texture.c:1727 si_texture_transfer_map - falhou ao criar textura temporária para manter cópia "untiled"
982459 (https://bugs.debian.org/982459)	mdadm	mdadm --examine em chroot sem /proc,/dev,/sys montados corrompe sistemas de arquivos do hospedeiro
981054 (https://bugs.debian.org/981054)	openipmi	openipmi: falta dependência em kmod
948318 (https://bugs.debian.org/948318)	openssh-server	openssh-server: incapaz de reiniciar "sshd restart" depois da atualização para a versão 8.1p1-2
991151 (https://bugs.debian.org/991151)	procps	procps: removida a opção "reload" do script de inicialização, quebrando corekeeper
989103 (https://bugs.debian.org/989103)	pulseaudio	pulseaudio regrediu na configuração control = Wave
984580 (https://bugs.debian.org/984580)	libpython3.9-dev	libpython3.9-dev: falta dependência em zlib1g-dev
990417 (https://bugs.debian.org/990417)	src:qemu	openjdk-11-jre-headless: executar java em qemu s390 provoca SIGILL at C [linux-vdso64.so.1 + 0x6f8] __kernel_getcpu + 0x8
859926 (https://bugs.debian.org/859926)	speech-dispatcher	quebra com pulse-audio como saída quando iniciado por speechd-up a partir do sistema de inicialização
932501 (https://bugs.debian.org/932501)	src:squid-deb-proxy	squid-deb-proxy: daemon não inicia devido ao arquivo de configuração não ser permitido pelo apparmor
991588 (https://bugs.debian.org/991588)	tpm2-abrmd	tpm2-abrmd não deveria usar Requires = systemd-udev-settle.service em sua "unit"

Número do bug	Pacote (fonte ou binário)	Descrição
991939 (https://bugs.debian.org/991939)	libjs-bootstrap4	libjs-bootstrap4: ligações simbólicas quebradas: /usr/share/javascript/bootstrap4/css/bootstrap*.css.map -> ../../../nodejs/bootstrap/dist/css/bootstrap*.c
991822 (https://bugs.debian.org/991822)	src:wine	src:wine: dh_auto_clean deleta arquivos não relacionados fora do pacote fonte
988477 (https://bugs.debian.org/988477)	src:xen	xen-hypervisor-4.14-amd64: xen dmesg exibe (XEN) AMD-Vi: IO_PAGE_FAULT on sata pci device
991788 (https://bugs.debian.org/991788)	xfce4-settings	xfce4-settings: tela preta depois de suspender quando a tela do notebook é fechada e reaberta

Capítulo 6

Mais informações sobre o Debian

6.1 Leitura complementar

Além destas notas de lançamento e do guia de instalação, mais documentação sobre o Debian está disponível a partir do Projeto de Documentação Debian (DDP), cujo objetivo é criar documentação de alta qualidade para usuários e desenvolvedores Debian, tal como a Referência Debian, o Guia de Novos Mantenedores Debian, o Debian FAQ e muito mais. Para todos os detalhes dos recursos existentes veja o site web de Documentação do Debian (`https://www.debian.org/doc/`) e o site web do Wiki do Debian (`https://wiki.debian.org/`).

Documentação para pacotes individuais é instalada em `/usr/share/doc/`*`pacote`*. Isso pode incluir informação de copyright, detalhes específicos do Debian e documentação do autor do software.

6.2 Obtendo ajuda

Há várias fontes de ajuda, aconselhamento e suporte para usuários Debian, no entanto, essas só deveriam ser consideradas depois de pesquisar a questão na documentação disponível. Esta seção fornece uma pequena introdução para essas fontes que podem ser úteis para novos usuários Debian.

6.2.1 Listas de discussão

As listas de discussão de maior interesse para usuários Debian são as listas debian-user (em inglês) e outras listas debian-user-*idioma* (para outros idiomas). Por exemplo, a debian-user-portuguese (`http://lists.debian.org/debian-user-portuguese`) para usuários que falam o idioma português do Brasil. Para informações sobre essas listas e detalhes sobre como se inscrever, veja `https://lists.debian.org/`. Por favor, verifique no histórico de mensagens se já existem respostas para suas perguntas antes de enviar algo e também respeite a etiqueta padrão para listas.

6.2.2 Internet Relay Chat

O Debian possui um canal IRC dedicado para o suporte e ajuda de usuários Debian, localizado na rede de IRC OFTC. Para acessar o canal, aponte seu cliente de IRC favorito para irc.debian.org e entre no canal `#debian` (em inglês). Também é possível usar o canal `#debian-br` para obter suporte em português do Brasil.

Por favor, siga as regras de conduta do canal, respeitando os outros usuários. As regras de conduta estão disponíveis no Wiki do Debian (`https://wiki.debian.org/DebianIRC`).

Para mais informações sobre a OFTC, por favor, visite o site web (`http://www.oftc.net/`).

6.3 Relatando bugs

Nos empenhamos para tornar o Debian um sistema operacional de alta qualidade; porém, isso não significa que os pacotes que disponibilizamos sejam totalmente livres de bugs. Coerentes com a filosofia de “desenvolvimento aberto” do Debian e como um serviço aos nossos usuários, nós fornecemos toda a

informação sobre bugs relatados em nosso próprio Sistema de Rastreamento de Bugs (BTS). O BTS pode ser acessado em https://bugs.debian.org/.

Caso você encontre um bug na distribuição ou no software empacotado que faz parte dela, por favor, relate-o para que possa ser corrigido adequadamente em futuros lançamentos. Para relatar bugs é necessário um endereço de e-mail válido. Nós pedimos isso para que possamos seguir os bugs e os desenvolvedores possam entrar em contato com quem os submeteu, caso seja necessário obter informação adicional.

Você pode submeter um relatório de bug utilizando o programa **reportbug** ou manualmente usando e-mail. Você pode descobrir mais a respeito do Sistema de Rastreamento de Bugs (BTS) e como utilizá-lo lendo a documentação de referência (disponível em /usr/share/doc/debian, caso você tenha instalado o doc-debian) ou online no Sistema de Rastreamento de Bugs (https://bugs.debian.org/).

6.4 Contribuindo para o Debian

Você não precisa ser um especialista para contribuir com o Debian. Ao ajudar outros usuários com problemas nas várias listas (https://lists.debian.org/) de suporte a usuário você está contribuindo com a comunidade. Identificar (e também resolver) problemas relacionados com o desenvolvimento da distribuição através da participação nas listas (https://lists.debian.org/) de desenvolvimento é também extremamente útil. Para manter a alta qualidade da distribuição Debian, submeta relatórios de bugs (https://bugs.debian.org/) e ajude os desenvolvedores a encontrá-los e a corrigi-los. A ferramenta how-can-i-help ajuda você a encontrar bugs relatados adequados para trabalhar. Caso você tenha jeito com as palavras então pode contribuir mais ativamente ajudando a escrever documentação (https://www.debian.org/doc/vcs) ou traduzir (https://www.debian.org/international/) a documentação existente para o seu próprio idioma.

Caso você possa dedicar mais tempo, poderá administrar uma parte da coleção de Software Livre dentro do Debian. É especialmente útil se as pessoas adotarem ou mantiverem itens que foram pedidos para serem incluídos no Debian. A base de dados de Pacotes Possíveis e que Necessitam de Trabalho (https://www.debian.org/devel/wnpp/) detalha essa informação. Caso você tenha interesse em grupos específicos então poderá achar agradável contribuir para alguns dos subprojetos (https://www.debian.org/devel/#projects) do Debian que incluem portes para arquiteturas específicas e Misturas Puras do Debian ("Debian Pure Blends") (https://wiki.debian.org/DebianPureBlends) para grupos específicos de usuários, entre muitos outros.

Em todo caso, se você estiver trabalhando na comunidade de software livre de qualquer forma, como utilizador, programador, escritor ou tradutor, você já está ajudando o esforço do software livre. A contribuição é recompensadora e divertida, além disso permite-lhe conhecer novas pessoas, dando-lhe aquela estranha sensação calorosa por dentro.

Capítulo 7

Glossário

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 Blu-ray Disc

DNS
: Domain Name System

DVD
: Digital Versatile Disc

GIMP
: GNU Image Manipulation Program

GNU
: GNU's Not Unix

GPG
: GNU Privacy Guard

LDAP
: Lightweight Directory Access Protocol

LSB
: Linux Standard Base

LVM
: Logical Volume Manager

MTA
: Mail Transport Agent

NBD
: Network Block Device

NFS
: Network File System

NIC
: Network Interface Card

NIS
: Network Information Service

PHP
: PHP: Hypertext Preprocessor

RAID
: Redundant Array of Independent Disks

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

Apêndice A

Gerenciando seu sistema buster antes da atualização

Este apêndice contém informações sobre como assegurar-se de que você consegue instalar ou atualizar pacotes da buster antes de atualizar para a bullseye. Isso só será necessário em situações específicas.

A.1 Atualizando seu sistema buster

Basicamente, isso não é diferente de qualquer outra atualização do buster que você tenha feito. A única diferença é que você precisa ter certeza de que sua lista de pacotes ainda contém referências para o buster conforme explicado em Seção A.2.

Caso você atualize o seu sistema usando um espelho Debian, ele automaticamente será atualizado para a última versão pontual do buster.

A.2 Verificando seus arquivos source-list do APT

Se qualquer uma das linhas nos seus arquivos source-list do APT (veja sources.list(5) (`https://manpages.debian.org//bullseye/apt/sources.list.5.html`)) contiver referências a "`stable`", você já está efetivamente "apontando" para a bullseye. Isso pode não ser o que você quer caso você ainda não esteja pronto para a atualização. Caso você já tenha executado **apt update**, você ainda pode voltar atrás sem problemas seguindo o procedimento abaixo.

Caso você também já tenha instalado pacotes do bullseye, provavelmente não há razão para instalar pacotes do buster. Neste caso, você terá que decidir por você mesmo se quer continuar ou não. É possível rebaixar a versão dos pacotes ("downgrade"), mas isso não é abordado neste documento.

Como root, abra o arquivo source-list do APT relevante (tal como `/etc/apt/sources.list`) com seu editor favorito, e verifique todas as linhas começando com `deb http:`, `deb https:`, `deb tor+http:`, `deb tor+https:`, `URIs: http:`, `URIs: https:`, `URIs: tor+http:` ou `URIs: tor+https:` para determinar se existe uma referência a "`stable`". Caso você encontre qualquer uma, altere de `stable` para `buster`.

Caso você tenha linhas começando com `deb file:` ou `URIs: file:`, você mesmo terá que verificar por você mesmo se o local indicado contém um repositório da buster ou da bullseye.

> IMPORTANTE
>
> Não mude nenhuma linha que comece com `deb cdrom:` ou `URIs: cdrom:`. Fazer isso invalidaria a linha e você teria que executar o **apt-cdrom** novamente. Não se preocupe se uma linha para uma fonte do tipo `cdrom:` apontar para "`unstable`". Embora confuso, isso é normal.

Caso você tenha feito quaisquer mudanças, salve o arquivo e execute

```
# apt update
```

para atualizar a lista de pacotes.

A.3 Removendo arquivos de configuração obsoletos

Antes de atualizar o seu sistema para bullseye, é recomendado remover arquivos de configuração antigos (tais como arquivos `*.dpkg-{new,old}` em `/etc`) do sistema.

Apêndice B

Colaboradores das notas de lançamento

Várias pessoas ajudaram com as notas de lançamento, incluindo, mas não se limitando a:

Adam D. Barratt, Adam Di Carlo, Andreas Barth, Andrei Popescu, Anne Bezemer, Bob Hilliard, Charles Plessy, Christian Perrier, Christoph Berg, Daniel Baumann, David Prévot, Eddy Petrișor, Emmanuel Kasper, Esko Arajärvi, Frans Pop, Giovanni Rapagnani, Gordon Farquharson, Hideki Yamane, Holger Wansing, Javier Fernández-Sanguino Peña, Jens Seidel, Jonas Meurer, Jonathan Nieder, Joost van Baal-Ilić, Josip Rodin, Julien Cristau, Justin B Rye, LaMont Jones, Luk Claes, Martin Michlmayr, Michael Biebl, Moritz Mühlenhoff, Niels Thykier, Noah Meyerhans, Noritada Kobayashi, Osamu Aoki, Paul Gevers, Peter Green, Rob Bradford, Samuel Thibault, Simon Bienlein, Simon Paillard, Stefan Fritsch, Steve Langasek, Steve McIntyre, Tobias Scherer, victory, Vincent McIntyre e W. Martin Borgert.

Este documento foi traduzido em vários idiomas. Muito obrigado aos tradutores!

Traduzido para português do Brasil por: Adriano Rafael Gomes, Chanely Marques, Daniel Lenharo, Éverton Arruda, Felipe Augusto van de Wiel e Marcelo Santana.

Índice Remissivo

A
Apache, 5

B
BIND, 5

C
Calligra, 3
Cryptsetup, 5

D
DocBook XML, 2
Dovecot, 5

E
Exim, 5

G
GCC, 5
GIMP, 5
GNOME, 3
GNUcash, 4
GnuPG, 5

I
Inkscape, 5

K
KDE, 3

L
LibreOffice, 3
LXDE, 3
LXQt, 3

M
MariaDB, 5
MATE, 3

N
Nginx, 5

O
OpenJDK, 5
OpenSSH, 5

P
packages
- apt, 2, 17, 29
- apt-listchanges, 21
- aptitude, 14, 20, 24
- aufs-dkms, 34
- bsd-mailx, 31
- ca-certificates-java, 35
- chef, 34
- cinder-volume, 28
- connman, 34
- cron, 35
- cups-browsed, 5
- cups-daemon, 5
- cups-filters, 5
- dblatex, 2
- debian-goodies, 20
- debian-kernel-handbook, 24
- debian-security-support, 32
- doc-debian, 40
- docbook-xsl, 2
- dpkg, 2
- drdsl, 34
- exfat-fuse, 7
- exfat-utils, 7
- exfatprogs, 7
- fail2ban, 31, 35
- firmware-iwlwifi, 31
- fuse, 29
- fuse3, 29
- gcc-10-base, 35
- gir1.2-diodon-1.0, 35
- gir1.2-gtd-1.0, 36
- git-el, 35
- glibc, 28
- gnome-control-center, 33
- gparted, 36
- grub2, 33
- guile-2.2-libs, 31
- gvfs-fuse, 29
- how-can-i-help, 40
- ibod, 34
- ifenslave, 36
- initramfs-tools, 12, 23
- intel-microcode, 31
- ipp-usb, 5, 6
- isdnactivecards, 34
- isdnutils, 34
- kio-fuse, 29
- libappindicator-dev, 34
- libappindicator1, 34
- libappindicator3-1, 34
- libayatana-appindicator, 34
- libgc1c2, 31
- libjs-bootstrap4, 37
- libnss-nis, 28
- libnss-nisplus, 28
- libpam-chroot, 36
- libpython3.9-dev, 36
- libsane1, 5, 6
- lilo, 33
- linux-image-*, 23
- linux-image-amd64, 24
- linux-source, 24
- localepurge, 20
- mailman, 33
- mailman3, 33
- mailman3-full, 33

mailutils, 31
mariadb-server-10.5,galera-4, 35
mdadm, 36
network-manager, 34
nova-compute, 28
openipmi, 36
openssh-server, 31, 36
openvswitch, 32
popularity-contest, 20
procps, 36
pulseaudio, 36
python-pkg-resources, 35
python-setuptools, 34
rails, 30
rdiff-backup, 31
redmine, 30
release-notes, 1
rsync, 28
rsyslog, 6
sane-airscan, 5
sendmail, 29
slapd, 34
speech-dispatcher, 36
src:gcc-10, 35
src:llvm-toolchain-11, 36
src:qemu, 36
src:squid-deb-proxy, 36
src:wine, 37
src:xen, 37
sshfs, 29
synaptic, 14
systemd, 7
tinc, 13
tpm2-abrmd, 36
udev, 23, 31
unbound, 28
upgrade-reports, 1
usrmerge, 34
vim, 28
vim-addon-manager, 28
vim-scripts, 28
wicd, 34
xfce4-settings, 37
xmlroff, 2
xsltproc, 2
Perl, 5
PHP, 5
Postfix, 5
PostgreSQL, 5

X

Xfce, 3