Note di rilascio per Debian 11 (bullseye), System z

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

17 aprile 2024

Indice

Capitolo 1

Introduzione

Questo documento fornisce informazioni agli utenti della distribuzione Debian sui cambiamenti principali nella versione 11 (nome in codice bullseye).

Le note di rilascio forniscono informazioni su come aggiornare in modo sicuro dalla versione 10 (nome in codice buster) alla versione attuale e informano gli utenti sui possibili problemi conosciuti in cui potrebbero incorrere durante tale processo.

È possibile ottenere la versione più recente di questo documento da `https://www.debian.org/releases/bullseye/releasenotes`.

ATTENZIONE

È impossibile elencare ogni possibile problema conosciuto, pertanto è stata fatta una selezione basata su probabili gravità e diffusione.

Si noti anche che vengono forniti solo il supporto e la documentazione relativi all'aggiornamento dalla versione precedente di Debian (in questo caso l'aggiornamento da buster). Se si deve aggiornare il sistema da versioni antecedenti, si suggerisce di leggere le edizioni precedenti delle note di rilascio e di aggiornare dapprima a buster.

1.1 Segnalare errori in questo documento

Si è cercato di verificare tutti i vari passi dell'aggiornamento descritti in questo documento e si è anche cercato di anticipare ogni possibile problema nel quale si potrebbe incorrere.

Ciononostante, se si ritiene di aver trovato un qualsiasi errore in questa documentazione (informazioni non corrette o mancanti), si invii una segnalazione al sistema di tracciamento dei bug (`https://bugs.debian.org/`) per il pacchetto `release-notes`. Prima di inviare la segnalazione si dovrebbe verificare se tra le segnalazioni d'errore esistenti (`https://bugs.debian.org/release-notes`) non sia già presente il problema trovato. Chiunque è libero di aggiungere delle informazioni alle segnalazioni esistenti in modo da contribuire al contenuto di questo documento.

Le segnalazioni con correzioni per i sorgenti del documento sono apprezzate e incoraggiate. In Sezione 1.3 sono disponibili ulteriori informazioni su come ottenere i sorgenti di questo documento.

1.2 Fornire resoconti di aggiornamento

Ogni informazione dagli utenti inerente l'aggiornamento da buster a bullseye è benvenuta. Se si desidera condividere informazioni, compilare una segnalazione nel sistema di tracciamento dei bug (`https://bugs.debian.org/`) per il pacchetto `upgrade-reports` con i risultati ottenuti. È richiesto che ogni eventuale allegato venga compresso usando **gzip**.

Quando si invia un resoconto di aggiornamento è necessario includere le seguenti informazioni:

- Lo stato del proprio database dei pacchetti prima e dopo l'aggiornamento: il database di `dpkg` dello stato dei pacchetti, disponibile in `/var/lib/dpkg/status` e le informazioni di `apt` sullo stato dei pacchetti, disponibili in `/var/lib/apt/extended_states`. Prima di aggiornare si dovrebbe aver effettuato una copia di sicurezza, come descritto in Sezione 4.1.1, ma è anche possibile trovare copie di `/var/lib/dpkg/status` in `/var/backups`.
- Le trascrizioni delle sessioni al terminale, ottenute con **script**, come descritto in Sezione 4.4.1.
- I registri di `apt`, disponibili in `/var/log/apt/term.log`, o i registri di **aptitude**, disponibili in `/var/log/aptitude`.

NOTA

Prima di inviare le informazioni contenute nei file di registro è opportuno verificare che non vi siano informazioni che si ritengono private, poiché tutta la segnalazione verrà inserita in un database pubblico.

1.3 Sorgenti di questo documento

I sorgenti di questo documento sono in formato DocBook XML . La versione in HTML viene generata usando `docbook-xsl` e `xsltproc`. La versione in PDF viene generata usando `dblatex` o `xmlroff`. I sorgenti delle note di rilascio sono disponibili nell'archivio Git del *Debian Documentation Project*. È possibile utilizzare l'interfaccia web (`https://salsa.debian.org/ddp-team/release-notes/`) per accedere ai singoli file tramite il web e vedere le rispettive modifiche. Per maggiori informazioni su come accedere a Git, consultare le pagine sul VCS del Debian Documentation Project (`https://www.debian.org/doc/vcs`).

Capitolo 2

Cosa c'è di nuovo in Debian 11

Il Wiki (https://wiki.debian.org/NewInBullseye) contiene ulteriori informazioni su questo argomento.

2.1 Architetture supportate

Le seguenti architetture sono ufficialmente supportate da Debian 11:

- PC a 32 bit (i386) e PC a 64 bit (amd64)
- ARM a 64 bit (arm64)
- ARM EABI (armel)
- ARMv7 (EABI hard-float ABI, armhf)
- MIPS little-endian (mipsel)
- MIPS little-endian a 64 bit (mips64el)
- PowerPC little-endian a 64 bit (ppc64el)
- IBM System z (s390x)

Maggiori informazioni sullo stato dei port e informazioni specifiche sul port per la propria architettura sono disponibili nelle pagine web relative ai port di Debian (https://www.debian.org/ports/).

2.2 Cosa c'è di nuovo nella distribuzione?

Ancora una volta la nuova versione di Debian contiene molto più software rispetto alla precedente, buster; la distribuzione include più di 11294 nuovi pacchetti, per un totale di oltre 59551 pacchetti. La maggior parte del software nella distribuzione è stata aggiornata: più di 42821 pacchetti software (corrispondenti al 72% di tutti i pacchetti in buster). Inoltre, un notevole numero di pacchetti (oltre 9519, il 16% dei pacchetti in buster) è stato rimosso dalla distribuzione per diversi motivi. Non ci saranno aggiornamenti per questi pacchetti ed essi saranno marcati come «obsoleti» nelle interfacce dei programmi di gestione dei pacchetti; vedere Sezione 4.8.

2.2.1 Desktop e pacchetti noti

Debian viene ancora una volta fornita con molti ambienti e applicazioni desktop. Fra l'altro include ora gli ambienti desktop GNOME 3.38, KDE Plasma 5.20, LXDE 11, LXQt 0.16, MATE 1.24 e Xfce 4.16.

Anche le applicazioni per la produttività sono state aggiornate, incluse le suite per l'ufficio:

- LibreOffice viene aggiornato alla versione 7.0;
- Calligra viene aggiornato a 3.2.

- GNUcash viene aggiornato a 4.4;

Fra i molti altri, questa versione include anche i seguenti aggiornamenti software:

Pacchetto	Versione in 10 (buster)	Versione in 11 (bullseye)
Apache	2.4.38	2.4.48
BIND Server DNS	9.11	9.16
Cryptsetup	2.1	2.3
Dovecot MTA	2.3.4	2.3.13
Emacs	26.1	27.1
Exim, server predefinito per la posta elettronica	4.92	4.94
GNU Compiler Collection come compilatore predefinito	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
la libreria C GNU	2.28	2.31
lighttpd	1.4.53	1.4.59
Immagine del kernel Linux	serie 4.19	serie 5.10
Insieme di strumenti LLVM/Clang	6.0.1 e 7.0.1 (predefinito)	9.0.1 e 11.0.1 (predefinito)
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
MTA Postfix	3.4	3.5
PostgreSQL	11	13
Python 3	3.7.3	3.9.1
Rustc	1.41 (1.34 per `armel`)	1.48
Samba	4.9	4.13
Vim	8.1	8.2

2.2.2 Scansione e stampa senza driver

Sia la stampa con `CUPS` sia la scansione con `SANE` sono sempre più spesso possibili senza la necessità di alcun driver (spesso non libero) specifico per il modello di hardware, specialmente nel caso di dispositivi messi in commercio negli ultimi 5 anni circa.

2.2.2.1 CUPS e stampa senza driver

Le moderne stampanti connesse via Ethernet o wireless possono già utilizzare la stampa senza driver (`https://wiki.debian.org/CUPSQuickPrintQueues`), implementata via `CUPS` e `cups-filters`, come era descritto nelle Note di rilascio per buster (`https://www.debian.org/releases/buster/amd64/release-notes/ch-whats-new.html#driverless-printing`). Debian 11 «bullseye» porta il nuovo pacchetto `ipp-usb`, che è raccomandato da `cups-daemon` e usa il protocollo IPP-over-USB (`https://wiki.debian.org/CUPSDriverlessPrinting#ippoverusb`) indipendente dal produttore supportato da molte stampanti moderne. Ciò permette ad un dispositivo USB di essere trattato come un dispositivo di rete, estendendo la stampa senza driver per includere le stampanti connesse via USB. Le specifiche sono descritte nel wiki (`https://wiki.debian.org/CUPSDriverlessPrinting#ipp-usb`).

Il file del servizio per systemd incluso nel pacchetto `ipp-usb` avvia il demone `ipp-usb` quando viene collegata una stampante USB, rendendola perciò disponibile per la stampa. In modo predefinito `cups-browsed` dovrebbe configurarla automaticamente, oppure può essere configurata manualmente con una coda di stampa senza driver locale (`https://wiki.debian.org/SystemPrinting`).

2.2.2.2 SANE e scansione senza driver

Il backend SANE officiale senza driver "driverless" è fornito da sane-escl in libsane1. Un backend senza driver sviluppato in modo indipendente è sane-airscan. Entrambi i backend gestiscono il protocollo eSCL (https://wiki.debian.org/SaneOverNetwork#escl) ma sane-airscan può anche usare il protocollo WSD (https://wiki.debian.org/SaneOverNetwork#wsd). Gli utenti dovrebbero prendere in considerazione l'idea di avere entrambi i backend sul proprio sistema.

eSCL e WSD sono protocolli di rete. Di conseguenza operano attraverso una connessione USB se il dispositivo è un dispositivo IPP-over-USB. Notare che libsane1 ha ipp-usb come pacchetto raccomandato. Ciò fa sì che un dispositivo adatto venga automaticamente impostato per usare un driver di backend "driverless" quando è connesso ad una porta USB.

2.2.3 Nuovo comando open generico

È disponibile un nuovo comando **open** come alias di comodità per **xdg-open** (in modo predefinito) o **run-mailcap**, gestito dal sistema update-alternatives(1) (https://manpages.debian.org//bullseye/dpkg/update-alternatives.1.html). È pensato per l'uso interattivo dalla riga di comando, per aprire file con la loro applicazione predefinita che può essere un programma grafico, quando disponibile.

2.2.4 Control groups v2

In bullseye systemd usa in modo predefinito cgroupv2 (gruppi di controllo v2) che fornisce una gerarchia unificata per il controllo di risorse. Sono disponibili parametri per la riga di comando del kernel per riabilitare i vecchi croups, se necessario; vedere le note per OpenStack nella sezione Sezione 5.1.8.

2.2.5 Registro ("Journal") di systemd persistente

Systemd in bullseye attiva in modo predefinito la sua funzionalità di log di registro persistente, archiviando i suoi file in /var/log/journal/. Vedere systemd-journald.service(8) (https://manpages.debian.org//bullseye/systemd/systemd-journald.service.8.html) per i dettagli; notare che in Debian il giornale è leggibile per i membri di adm, in aggiunta al gruppo predefinito systemd-journal.

Ciò non dovrebbe interferire con alcun demone per registrazione di log tradizionale esistente, come rsyslog, ma per gli utenti che non utilizzano funzionalità speciali di un demone simile può essere desiderabile disinstallarlo e passare ad usare solo il journaling.

2.2.6 Nuovo metodo di input Fcitx 5

Fcitx 5 è un metodo di input per cinese, giapponese, coreano e molte altre lingue. È il successore del popolare Fcitx 4 in buster. La nuova versione supporta Wayland e ha una migliore gestione degli addon. Ulteriori informazioni, inclusa la guida alla migrazione, possono essere trovate nel wiki (https://wiki.debian.org/I18n/Fcitx5).

2.2.7 Novità dal Blend Debian Med

Il Team Debian Med ha preso parte alla lotta contro il COVID-19 pacchettizzando software per ricerca sul virus a livello di sequenza e per la lotta alla pandemia con gli strumenti usati in epidemiologia. Lo sforzo continuerà nel prossimo ciclo di rilascio, con attenzione agli strumenti di apprendimento macchina che sono usati in entrambi i campi.

Oltre all'aggiunta di nuovi pacchetti nel campo delle scienze della vita e della medicina, sempre più pacchetti esistenti hanno ottenuto il supporto per l'Integrazione Continua.

Una gamma di applicazioni critiche per le prestazioni traggono ora beneficio da SIMD Everywhere (https://wiki.debian.org/SIMDEverywhere). Questa libreria permette ai pacchetti di essere disponibili su più piattaforme hardware supportate da Debian (in particolare su arm64), mantenendo al contempo il beneficio in termini di prestazioni fornito dai processori che supportano estensioni vettoriali, come AVX su amd64 o NEON su arm64.

Per installare i pacchetti mantenuti dal team Debian Med, installare i metapacchetti chiamati med-* che sono alla versione 3.6.x per Debian bullseye. Visitare le pagine delle attività Debian Med (http:

//blends.debian.org/med/tasks) per vedere l'intera gamma del software per biologia e medicina disponibile in Debian.

2.2.8 Supporto del kernel per exFAT

bullseye è il primo rilascio a fornire un kernel Linux che ha il supporto per il file system exFAT e lo usa in modo predefinito per montare file system exFAT. Di conseguenza non è più necessario usare l'implementazione di file system in spazio utente fornita con il pacchetto `exfat-fuse`. Se si desidera continuare ad utilizzare l'implementazione di file system in spazio utente, è necessario invocare lo strumento ausiliario **mount.exfat-fuse** direttamente quando si monta un file system exFAT.

Strumenti per creare e verificare un file system exFAT sono forniti nel pacchetto `exfatprogs` dagli autori dell'implementazione exFAT per il kernel Linux. L'implementazione indipendente di questi strumenti fornita con il pacchetto esistente `exfat-utils` è sempre disponibile, ma non può essere installata insieme alla nuova implementazione. È raccomandato migrare al pacchetto `exfatprogs`, anche se si devono controllare e modificare le opzioni del comando che sono molto probabilmente non compatibili.

2.2.9 Traduzioni delle pagine di manuale migliorate

Le pagine di manuale di diversi progetti, come systemd, util-linux, OpenSSH e Mutt sono state sostanzialmente migliorate in diverse lingue, incluse francese, spagnolo e macedone. Per sfruttare questi miglioramenti, installare `manpages-`*xx* (dove *xx* è il codice della lingua che si preferisce).

Durante il ciclo di vita del rilascio bullseye, i backport di ulteriori miglioramenti delle traduzioni verranno forniti attraverso l'archivio `backports`.

2.2.10 Gestione migliorata di sistemi init alternativi

Il sistema init predefinito in Debian è `systemd`. In bullseye sono gestiti diversi sistemi init alternativi (come init in stile System-V e OpenRC) e la maggior parte degli ambienti desktop ora funziona bene nei sistemi che eseguono init alternativi. Dettagli su come cambiare sistema init (e dove trovare aiuto per i problemi relativi all'esecuzione di init diversi da systemd) sono disponibili nel wiki Debian (`https://wiki.debian.org/Init`).

2.2.11 Initial availability of the Bazel build system

The Bazel build system (`https://bazel.build/`) is available in Debian starting with this release. This is a bootstrap variant that doesn't include local versions of the extended Bazel ecosystem. However, the current package does provide identical functionality to core upstream Bazel, with the advantage of convenient Debian package management for the installation. While building Debian packages is not currently recommended yet, any software that supports Bazel builds should build normally using the `bazel-bootstrap` package. This includes build-time downloads of required dependencies.

The Debian Bazel Team (`https://salsa.debian.org/bazel-team/meta`) is working to package an extensible version of Bazel for future Debian releases. This extensible version will allow additional components of the Bazel ecosystem to be included as native Debian packages. More importantly, this version will allow Debian packages to be built using Bazel. Contributions to the team are welcome!

Capitolo 3

Sistema d'installazione

L'installatore Debian è il sistema d'installazione ufficiale per Debian. Offre molti metodi d'installazione, la cui disponibilità dipende dall'architettura del proprio sistema.

Le immagini dell'installatore per bullseye possono essere trovate, insieme alla guida all'installazione, sul sito web di Debian (`https://www.debian.org/releases/bullseye/debian-installer/`).

La guida all'installazione è inclusa anche nel primo elemento dei set ufficiali dei DVD (CD/blu-ray) Debian, in:

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

Si possono anche verificare le errata corrige (`https://www.debian.org/releases/bullseye/debian-installer/index#errata`) dell'installatore Debian per un elenco di problematiche note.

3.1 Cosa c'è di nuovo nel sistema di installazione?

L'installatore Debian ha fatto molti passi avanti dalla precedente versione rilasciata ufficialmente con Debian 10, raggiungendo un migliore supporto all'hardware e alcune nuove e interessanti funzionalità e migliorie.

Per una panoramica dei dettagli delle modifiche da buster, consultare gli annunci dei rilasci beta e RC di bullseye, disponibili nella cronologia delle notizie dell'installatore Debian (`https://www.debian.org/devel/debian-installer/News/`).

3.1.1 Aiuto per l'installazione di firmware

Sempre più spesso i dispositivi periferici richiedono il caricamento di firmware come parte dell'inizializzazione dell'hardware. Per aiutare ad affrontare questo problema l'installatore ha una nuova funzionalità. Se dell'hardware installato richiede l'installazione di file firmware, l'installatore cerca di aggiungerli al sistema sulla base di una mappatura da ID hardware a nomi di file di firmware.

Questa nuova funzionalità è limitata alle immagini non ufficiali dell'installatore con incluso il firmware (vedere https://www.debian.org/releases/bullseye/debian-installer/#firmware_nonfree (`https://www.debian.org/releases/bullseye/debian-installer/#firmware_nonfree`)). Il firmware solitamente non è conforme alle DFSG, perciò non è possibile distribuirlo nel repository principale Debian.

Se si incontrano problemi relativi a firmware (mancante), leggere il capitolo dedicato della guida di installazione (`https://www.debian.org/releases/bullseye/amd64/ch06s04#completing-installed`

3.1.2 Installazione automatizzata

Alcuni implicano anche modifiche al supporto nell'installatore per installazioni automatizzate con l'uso di file di preconfigurazione. Ciò significa che se si possiedono file preconfigurati che funzionavano con l'installatore di buster non ci si può attendere che questi funzionino senza modifiche anche con il nuovo installatore.

La Guida all'installazione (`https://www.debian.org/releases/bullseye/installmanual`) include un'appendice separata aggiornata con una documentazione estesa sull'uso di preconfigurazioni.

3.2 Immagini per contenitori e macchine virtuali

Immagini contenitore per Debian bullseye multi-architettura sono disponibili su Docker Hub (`https://hub.docker.com/_/debian`). In aggiunta alle immagini standard è disponibile una variante «slim» che riduce l'uso del disco.

Immagini di macchine virtuali per il gestore di VM Hashicorp Vagrant sono pubblicate nel Vagrant Cloud (`https://app.vagrantup.com/debian`).

Capitolo 4

Aggiornamenti da Debian 10 (buster)

4.1 Preparazione all'aggiornamento

Prima di procedere all'aggiornamento si consiglia di leggere anche le informazioni contenute in Capitolo 5, dove vengono trattati i potenziali problemi non direttamente collegati al processo di aggiornamento, ma che potrebbe essere comunque importante conoscere prima di iniziare.

4.1.1 Salvare i dati e le informazioni di configurazione

Prima di aggiornare il proprio sistema si raccomanda di effettuare un salvataggio completo o quantomeno una copia di sicurezza di tutti quei dati e quelle informazioni di configurazione che non ci si può permettere di perdere. Gli strumenti e i processi di aggiornamento sono abbastanza affidabili, ma un problema dell'hardware durante l'aggiornamento potrebbe generare un sistema fortemente danneggiato.

Le cose principali che si potrebbe considerare di salvare sono i contenuti di `/etc`, `/var/lib/dpkg`, `/var/lib/apt/extended_states` e l'output di `dpkg --get-selections "*"` (le virgolette sono importanti). Se si usa **aptitude** per gestire i pacchetti, si dovrebbe salvare anche `/var/lib/aptitude/pkgstates`.

Il processo di aggiornamento in quanto tale non modifica nulla nelle directory `/home`, tuttavia alcune applicazioni (come ad esempio alcune parti della suite Mozilla e gli ambienti desktop GNOME e KDE) sovrascrivono le impostazioni dell'utente preesistenti con i nuovi valori predefiniti quando un utente avvia per la prima volta la nuova versione dell'applicazione. Per precauzione si potrebbe quindi voler fare una copia di sicurezza dei file e delle directory nascosti («dotfile», cioè file i cui nomi iniziano con un punto) che si trovano nelle directory «home» degli utenti. Tale copia potrebbe aiutare a ripristinare o a ricreare le vecchie impostazioni. Potrebbe anche essere il caso di informare gli utenti su questo argomento.

Tutte le installazioni di pacchetti devono essere eseguite con i privilegi di superutente, per cui è necessario effettuare il login come utente `root`, oppure usare **su** o **sudo**, per ottenere i diritti d'accesso necessari.

L'aggiornamento ha alcune condizioni preliminari; prima di eseguirlo si dovrebbe verificarle.

4.1.2 Informare gli utenti in anticipo

È saggio informare in anticipo tutti gli utenti di qualunque aggiornamento si stia pianificando, anche se gli utenti che accedono al sistema tramite una connessione **ssh** non dovrebbero notare granché durante l'aggiornamento e dovrebbero poter continuare a lavorare.

Se si desidera prendere delle precauzioni supplementari, si esegua un salvataggio delle partizioni degli utenti (`/home`) o le si smonti prima di aggiornare il sistema.

Con l'aggiornamento a bullseye si dovrà anche fare un aggiornamento del kernel, per cui sarà necessario riavviare il sistema. Tipicamente ciò verrà fatto dopo che l'aggiornamento è terminato.

4.1.3 Preparazione all'indisponibilità dei servizi

Tra i pacchetti interessati all'aggiornamento ce ne potrebbero essere alcuni a cui sono associati dei servizi. In questo caso, tali servizi saranno fermati mentre è in corso la sostituzione o la configurazione dei pacchetti. In questo periodo di tempo i servizi non saranno disponibili.

La durata del disservizio varia a seconda del numero di pacchetti da aggiornare sul sistema e comprende anche il tempo che occorre all'amministratore di sistema per rispondere alle domande sulla configurazione poste dall'aggiornamento dei pacchetti. Notare che se l'aggiornamento non è presidiato e il sistema richiede una risposta per andare avanti è probabile che i servizi rimangano non disponibili[1] per un periodo di tempo considerevole.

Se il sistema in fase di aggiornamento fornisce servizi critici per gli utenti o la rete[2], è possibile ridurre il tempo di disservizio facendo un aggiornamento minimo, come descritto in Sezione 4.4.4, seguito da un aggiornamento del kernel, un riavvio e poi l'aggiornamento dei pacchetti associati ai servizi critici. Fare l'aggiornamento di questi pacchetti prima di fare l'aggiornamento completo descritto in Sezione 4.4.5. Questo metodo assicura che i servizi critici restino in funzione mentre è in corso l'aggiornamento completo del sistema e che il periodo di disservizio sia breve.

4.1.4 Preparazione per il ripristino

Sebbene Debian cerchi di garantire che il sistema rimanga sempre in uno stato avviabile, c'è sempre la possibilità che si abbiano problemi a riavviare il sistema dopo l'aggiornamento. I potenziali problemi che sono noti sono documentati in questo e nei prossimi capitoli delle presenti note di rilascio.

Pertanto è sensato assicurarsi di essere in grado di ripristinare il proprio sistema se questo non riesce a riavviarsi o a tirare su la rete, se è gestito da remoto.

Se si sta aggiornando da remoto tramite una connessione **ssh** è fortemente raccomandato prendere tutte le precauzioni necessarie per essere in grado di accedere al server tramite un terminale seriale remoto. È possibile che, dopo l'aggiornamento del kernel e il riavvio del sistema, si debba sistemare la configurazione del sistema tramite una console locale. Analogamente, se il sistema viene accidentalmente riavviato nel mezzo di un aggiornamento è possibile che lo si debba ripristinare usando una console locale.

Per il ripristino d'emergenza generalmente viene raccomandato di usare è la *modalità di ripristino* dell'installatore di Debian bullseye. Il vantaggio di usare l'installatore consiste nel fatto che è possibile scegliere fra i suoi numerosi metodi per trovare quello che meglio corrisponde alla propria situazione. Per maggiori informazioni si consulti la sezione «Recupero di un sistema danneggiato» nel capitolo 8 della Guida all'installazione (`https://www.debian.org/releases/bullseye/installmanual`) e le FAQ dell'installatore di Debian (`https://wiki.debian.org/DebianInstaller/FAQ`).

Se questa operazione non riesce, sarà necessario trovare un modo alternativo per avviare il proprio sistema in modo da potervi accedere per ripararlo. Una possibilità è l'utilizzo di un'immagine di ripristino speciale o di installazione live (`https://www.debian.org/CD/live/`). Dopo aver avviato in tal modo, si dovrebbe essere in grado di montare il proprio file system radice ed entrarvi con **chroot** per trovare e correggere il problema.

4.1.4.1 Shell di debug durante l'avvio con initrd

Il pacchetto `initramfs-tools` include una shell di debug[3] negli initrd che genera. Per esempio, se initrd non è in grado di montare il file system radice si verrà rimandati in questa shell di debug, la quale mette a disposizione i comandi di base per trovare il problema e, se possibile, risolverlo.

Le cose di base da controllare sono: la presenza dei file device corretti in `/dev`, quali moduli vengono caricati (`cat /proc/modules`) e l'output di **dmesg** per gli errori durante il caricamento dei driver. L'output di **dmesg** mostra inoltre quali file device sono stati assegnati a quali dischi; questi risultati andranno confrontati con l'output di `echo $ROOT`, per assicurarsi che il file system radice sia sul device atteso.

Se si è riusciti a risolvere il problema, digitando `exit` si uscirà dalla shell di debug e si continuerà il processo di avvio a partire dal punto in cui il problema si è verificato. Naturalmente sarà anche

[1] Se la priorità di debconf è impostata ad un valore molto alto potrebbe bloccare i prompt di configurazione quindi i servizi che si basano su risposte predefinite che non sono appropriate per il proprio sistema non partiranno.

[2] Per esempio i servizi DNS e DHCP, in modo particolare se non c'è ridondanza o failover. Nel caso del DHCP gli utenti finali potrebbero essere disconnessi dalla rete se il lease time è inferiore al tempo necessario per la conclusione dell'aggiornamento.

[3] Questa funzionalità può essere disabilitata aggiungendo il parametro `panic=0` ai parametri di avvio del proprio sistema.

necessario risolvere il problema sottostante e rigenerare initrd in modo che il prossimo avvio non fallisca nuovamente.

4.1.4.2 Shell di debug durante l'avvio con systemd

Se l'avvio fallisce con systemd è possibile ottenere una shell root di debug cambiando la riga di comando del kernel. Se l'avvio di base ha successo, ma l'avvio di alcuni servizi fallisce, può essere utile aggiungere `systemd.unit=rescue.target` ai parametri del kernel.

Atrimenti il parametro `systemd.unit=emergency.target` del kernel fornirà una shell di root non appena possibile. Tuttavia ciò viene fatto prima del montaggio del file system radice con permessi in lettura e scrittura. Sarà necessario farlo manualmente con:

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

Ulteriori informazioni su come fare il debug di un avvio non funzionante con systemd possono essere trovate nell'articolo Diagnosing Boot Problems (`https://freedesktop.org/wiki/Software/systemd/Debugging/`).

4.1.5 Preparazione di un ambiente sicuro per l'aggiornamento

IMPORTANTE

Se si stanno usando alcuni servizi VPN (come `tinc`) tenere a mente che potrebbero non essere disponibili durante l'aggiornamento. Consultare Sezione 4.1.3.

Per ottenere un margine supplementare di sicurezza durante l'aggiornamento da remoto si suggerisce di eseguire i processi di aggiornamento nella console virtuale fornita dal programma **screen**, che consente la riconnessione sicura e garantisce che il processo di aggiornamento non venga interrotto nemmeno nel caso in cui il processo di connessione remota si interrompa temporaneamente.

4.2 Partire da una Debian «pura»

Il processo di aggiornamento descritto in questo capitolo è stato progettato per sistemi Debian stable «puri». APT controlla ciò che è installato nel sistema. Se la propria configurazione di APT fa riferimento a fonti aggiuntive oltre a buster o se si sono installati pacchetti da altri rilasci o da terze parti, allora per assicurare un processo di aggiornamento affidabile si potrebbe voler iniziare rimuovendo tali fattori di complicazione.

Il file di configurazione principale che APT utilizza per decidere da quali fonti scaricare i pacchetti è `/etc/apt/sources.list`, ma può anche utilizzare i file nella directory`/etc/apt/sources.list.d/`; per i dettagli vedere sources.list(5) (`https://manpages.debian.org//bullseye/apt/sources.list.5.html`). Se il proprio sistema sta utilizzando più file source-list allora sarà necessario assicurarsi che rimangano coerenti.

4.2.1 Aggiornamento a Debian 10 (buster)

L'aggiornamento diretto da rilasci Debian più vecchi di 10 (buster) non sono supportati. Si può visualizzare la propria versione di Debian con:

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

Seguire le istruzioni nelle Note di rilascio per Debian 10 (`https://www.debian.org/releases/buster/releasenotes`) per aggiornare prima a Debian 10.

4.2.2 Rimozione dei pacchetti non Debian

Di seguito vengono indicati due metodi per trovare pacchetti installati che non provengono da Debian, usando **aptitude** o **apt-forktracer**. Notare che nessuno dei due è accurato al 100% (per esempio, quello con aptitude elenca i pacchetti che erano una volta forniti da Debian ma che non lo sono più, come i vecchi pacchetti del kernel).

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

4.2.3 Aggiornare all'ultimo rilascio minore

Questa procedura presume che il proprio sistema sia stato aggiornato fino all'ultimo aggiornamento disponibile per buster. Se non è così o non si è sicuri, seguire le istruzioni contenute in Sezione A.1.

4.2.4 Preparare il database dei pacchetti

Si dovrebbe controllare che il database dei pacchetti sia a posto prima di procedere con l'aggiornamento. Se si usa un altro gestore di pacchetti come `aptitude` o `synaptic` controllare ogni azione in sospeso. Un pacchetto per cui è programmata l'installazione o la rimozione potrebbe interferire con il processo di aggiornamento. Si noti che la correzione di questa situazione è possibile solo se i propri file source-list per APT puntano tuttora a *buster* e non a *stable* o a *bullseye*. A tale proposito vedere Sezione A.2.

4.2.5 Rimuovere pacchetti obsoleti

È una buona idea rimuovere i pacchetti obsoleti dal proprio sistema prima dell'aggiornamento. Possono introdurre complicazioni durante il processo di aggiornamento e possono rappresentare rischi di sicurezza dato che non sono più mantenuti.

4.2.6 Ripulire i file di configurazione rimasti indietro

Un aggiornamento precedente può aver lasciato indietro copie inutilizzate dei file di configurazione: vecchie versioni di file di configurazione, versioni fornite dai manutentori dei pacchetti, ecc. La rimozione dei file lasciati da precedenti aggiornamenti può evitare confusioni. Trovare questi file rimasti indietro con:

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

4.2.7 La sezione "security" di sicurezza

Per le righe delle fonti di APT che si riferiscono all'archivio di sicurezza il formato è stato leggermente cambiato insieme al nome del rilascio passando da `buster/updates` a `bullseye-security`; vedere Sezione 5.1.2.

4.2.8 La sezione «proposed-updates» (aggiornamenti proposti)

Se la sezione `proposed-updates` è elencata nei propri file source-list per APT, la si dovrebbe rimuovere prima di tentare l'aggiornamento del sistema. Questa precauzione serve per ridurre il rischio di conflitti.

4.2.9 Fonti non ufficiali

Se si ha un qualsiasi pacchetto non-Debian nel proprio sistema, si presti attenzione al fatto che questi possono essere rimossi durante l'aggiornamento a causa di conflitti di dipendenze. Se questi pacchetti sono stati installati aggiungendo un archivio di pacchetti supplementare nei propri file source-list per APT, si dovrebbe controllare che tale archivio offra anche pacchetti compilati per bullseye e modificare di conseguenza la riga della fonte contemporaneamente alle righe delle fonti per i pacchetti Debian.

Alcuni utenti potrebbero avere installate nel proprio sistema buster versioni *non ufficiali* «più recenti» da backport di pacchetti che *sono* in Debian. Tali pacchetti sono i candidati più probabili a causare problemi durante un aggiornamento, in quanto potrebbero generare conflitti fra file[4]. Sezione 4.5 contiene alcune informazioni su come gestire i conflitti tra file nel caso si verifichino.

4.2.10 Disattivare il pinning di APT

Se si è configurato APT in modo da installare taluni pacchetti da una distribuzione diversa da stable (ad esempio da testing), si potrebbe dover modificare la configurazione del pinning del proprio APT (memorizzata in `/etc/apt/preferences` e `/etc/apt/preferences.d/`) in modo da consentire l'aggiornamento dei pacchetti alle versioni nel nuovo rilascio stable. Maggiori informazioni sul pinning di APT sono disponibili in apt_preferences(5) (`https://manpages.debian.org//bullseye/apt/apt_preferences.5.en.html`).

4.2.11 Verifica dello stato dei pacchetti

Si raccomanda di controllare dapprima lo stato di tutti i pacchetti e di verificare che tutti siano in uno stato aggiornabile, indipendentemente dal metodo usato per l'aggiornamento. Il comando seguente mostrerà tutti i pacchetti con uno stato «Half-Installed» o «Failed-Config» e quelli con un qualsiasi stato di errore.

```
# dpkg --audit
```

È anche possibile controllare lo stato di tutti i pacchetti sul proprio sistema usando **aptitude** o con comandi come ad esempio

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

o

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

È auspicabile la rimozione di qualsiasi blocco prima dell'aggiornamento. Se qualsiasi pacchetto essenziale per l'aggiornamento è bloccato («on hold») l'aggiornamento fallirà.

Si noti che **aptitude** usa un metodo differente per registrare i pacchetti bloccati rispetto ad **apt** e **dselect**. È possibile identificare i pacchetti bloccati per **aptitude** eseguendo

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

Se si desidera controllare quali pacchetti erano bloccati per **apt**, si dovrebbe eseguire

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

Se un pacchetto è stato modificato e ricompilato localmente, e non lo si è rinominato né vi si è aggiunto un numero di epoca nella versione, è necessario bloccarlo per impedire che venga aggiornato.

Lo stato «bloccato» di un pacchetto per **apt** può essere modificato eseguendo il comando:

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

Si sostituisca `hold` con `install` per rimuovere lo stato «bloccato» del pacchetto.

Se c'è bisogno di sistemare qualcosa è meglio controllare che i propri file source-list per APT puntino sempre a buster come illustrato in Sezione A.2.

4.3 Preparazione dei file source-list per APT

Prima di iniziare l'aggiornamento è necessario riconfigurare i file source-list di APT (`/etc/apt/sources.list` e i file in `/etc/apt/sources.list.d/`) per aggiungere fonti per `bullseye` e tipicamente per rimuovere le fonti per `buster`.

APT prenderà in considerazione tutti i pacchetti che possono essere trovati tramite qualsiasi archivio configurato e installerà il pacchetto con il numero di versione più alto, dando la priorità alle righe

[4] Normalmente il sistema di gestione di pacchetti di Debian non consente a un pacchetto di rimuovere o sostituire un file controllato da un altro pacchetto, a meno che non sia stato definito che il primo pacchetto sostituisce il secondo.

menzionate per prime. Perciò, nel caso in cui siano presenti più posizioni di mirror, elencare per prime quelle sull'hard disc locale, poi i CD-ROM e infine i mirror remoti.

Si fa spesso riferimento a un rilascio sia tramite il suo nome in codice (ad esempio `buster`, `bullseye`), sia tramite la denominazione del suo stato (cioè `oldstable`, `stable`, `testing`, `unstable`). Fare riferimento ad un rilascio attraverso il suo nome in codice presenta il vantaggio che non si sarà mai sorpresi da un nuovo rilascio, pertanto è il metodo qui adottato. Questo naturalmente significa che si dovrà prestare attenzione agli annunci di rilascio. Se invece si utilizza la denominazione dello stato, si vedrà una grande quantità di aggiornamenti disponibili per i propri pacchetti non appena avviene un rilascio.

Debian fornisce due mailing-list per gli annunci che aiutano a rimanere aggiornati sulle informazioni importanti relative ai rilasci di Debian:

- Iscrivendosi alla mailing-list degli annunci Debian (`https://lists.debian.org/debian-announce/`) si riceverà una notifica ogni volta che Debian fa un nuovo rilascio, ad esempio come quando `bullseye` passa da `testing` a `stable`.
- Iscrivendosi alla mailing-list degli annunci di sicurezza di Debian (`https://lists.debian.org/debian-security-announce/`) si riceverà una notifica ogni volta che Debian pubblica un annuncio di sicurezza.

4.3.1 Aggiunta di fonti internet per APT

Nelle nuove installazioni APT viene impostato in modo predefinito per utilizzare il servizio APT CDN di Debian che dovrebbe assicurare che i pacchetti vengano automaticamente scaricati da un server vicino in termini di rete. Dato che questo è un servizio relativamente nuovo le installazioni più vecchie possono avere configurazioni che puntano ancora ad uno dei server Internet principali di Debian o uno dei mirror. Se ancora non lo si è fatto, è raccomandato passare all'utilizzo del servizio CDN nella propria configurazione di APT.

Per utilizzare il servizio CDN aggiungere una riga come quella seguente alla propria configurazione delle fonti per APT (presupponendo di usare `main` e `contrib`):

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

Dopo aver aggiunto le nuove fonti, disabilitare le righe «`deb`» preesistenti ponendovi davanti un simbolo cancelletto (`#`).

Tuttavia se si hanno risultati migliori usando un mirror specifico che è vicino in termini di rete, tale opzione è ancora disponibile.

Gli indirizzi dei mirror di Debian sono reperibili in `https://www.debian.org/distrib/ftplist` (guardare la sezione «Elenco dei mirror Debian»).

Per esempio, si supponga che il proprio mirror Debian più vicino sia `http://mirrors.kernel.org`. Ispezionandolo con un browser web si noterà che le directory principali sono organizzate nel modo seguente:

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

Per configurare APT per l'utilizzo di un determinato mirror aggiungere una riga come la seguente (ancora una volta presumendo di utilizzare `main` e `contrib`):

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

Si noti che «`dists`» è aggiunto implicitamente e che gli argomenti che seguono il nome del rilascio sono utilizzati per espandere il percorso su directory multiple.

Di nuovo, dopo aver aggiunto le nuove fonti disabilitare le voci di archivio precedentemente esistenti.

4.3.2 Aggiunta di fonti per APT da mirror locale

Anziché usare mirror remoti dei pacchetti, si potrebbe voler modificare i file source-list di APT in modo da usare un mirror su un disco locale (eventualmente montato su NFS).

Per esempio, il proprio mirror dei pacchetti potrebbe essere in `/var/local/debian/` e avere le directory principali come segue:

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

Per poter utilizzare questo mirror con `apt`, si aggiunga questa riga al proprio `sources.list`:

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

Si noti che «`dists`» è aggiunto implicitamente e che gli argomenti che seguono il nome del rilascio sono utilizzati per espandere il percorso su directory multiple.

Dopo aver aggiunto le nuove fonti, disabilitare le voci di archivio preesistenti nei file source-list di APT, ponendovi davanti un simbolo cancelletto (`#`).

4.3.3 Aggiunta di fonti per APT da supporti ottici

Se si vogliono utilizzare *soltanto* DVD (o CD o dischi Blu-ray) si disabilitino, commentandole, le voci esistenti in tutti i file source-list di APT ponendovi davanti un simbolo cancelletto (`#`).

Ci si accerti che in `/etc/fstab` ci sia una riga che abiliti la possibilità di montare la propria unità CD-ROM nel punto di montaggio `/media/cdrom`. Per esempio, se l'unità del CD-ROM è `/dev/sr0`, `/etc/fstab` dovrebbe contenere una riga come la seguente:

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

Si noti che *non ci devono essere spazi* fra le parole `noauto,ro` nel quarto campo.

Per verificare il funzionamento, inserire un CD e provare a eseguire

```
# mount /media/cdrom    # questo monta il CD nel punto di montaggio
# ls -alF /media/cdrom  # questo dovrebbe mostrare la directory radice del CD
# umount /media/cdrom   # questo smonta il CD
```

Poi, si esegua:

```
# apt-cdrom add
```

per ciascun CD-ROM di binari di Debian che si possiede, al fine di aggiungere i dati di ciascun CD al database di APT.

4.4 Aggiornare i pacchetti

Il modo raccomandato per aggiornare da rilasci di Debian precedenti è quello di usare lo strumento do gestione dei pacchetti **apt**.

NOTA

apt è pensato per l'uso interattivo e non dovrebbe essere utilizzato in script. Negli script si dovrebbe usare **apt-get** che ha un output stabile più adatto per l'analisi semantica.

Non ci si dimentichi di montare tutte le partizioni necessarie (in particolare le partizioni radice e `/usr`) in modalità di lettura e scrittura, con un comando del tipo:

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

Si dovrebbe poi controllare molto attentamente che le voci sulle fonti di APT (in `/etc/apt/sources.list` e nei file in `/etc/apt/sources.list.d/`) facciano riferimento a «`bullseye`» o a «`stable`». Non ci dovrebbero essere voci per fonti che puntano a buster.

NOTA

Qualche volta le righe delle fonti per un CD-ROM potrebbero fare riferimento a «`unstable`»; sebbene ciò possa generare confusione *non* le si dovrebbe modificare.

4.4.1 Registrazione della sessione

È fortemente raccomandato l'utilizzo del programma **/usr/bin/script** per registrare una trascrizione della sessione di aggiornamento. In tal modo, se si verificasse un problema si disporrà di una registrazione di quanto accaduto e, se necessario, si potranno fornire le informazioni esatte in un'eventuale segnalazione di errori. Per avviare la registrazione, si digiti:

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

o un comando simile. Se fosse necessario fare la trascrizione di un'altra sessione (perché, per esempio, è necessario riavviare il sistema), usare valori diversi per *fase* in modo da indicare anche la fase dell'aggiornamento che si sta registrando. Non si collochi il file della registrazione in una directory temporanea come `/tmp` o `/var/tmp`, in quanto i file in queste directory potrebbero venir cancellati durante l'aggiornamento o durante un qualunque riavvio.

Il file generato permetterà anche di rileggere le informazioni scorse fuori dalla schermata. Se si usa la console di sistema, basterà passare a VT2 (con Alt + F2) e, dopo aver effettuato l'accesso, utilizzare il comando `less -R ~root/upgrade-bullseye.script` per visualizzare il file.

Dopo aver completato l'aggiornamento si può arrestare **script**, digitando `exit` al prompt.

apt mantiene anche un registro ("log") in `/var/log/apt/history.log` dei cambiamenti di stato dei pacchetti e dell'output del terminale in `/var/log/apt/term.log`. **dpkg**, in aggiunta, registra tutti i cambiamenti di stato dei pacchetti in `/var/log/dpkg.log`. Se si usa **aptitude**, anch'esso registra cambiamenti di stato in `/var/log/aptitude`.

Se si è utilizzato il parametro *-t* per **script**, si può utilizzare il programma **scriptreplay** per replicare l'intera sessione:

```
# scriptreplay ~/upgrade-bullseye-fase.time ~/upgrade-bullseye-fase.script
```

4.4.2 Aggiornamento della lista dei pacchetti

Anzitutto deve essere recuperata la lista dei pacchetti disponibili per la nuova versione. Lo si fa eseguendo:

```
# apt update
```

NOTA

Gli utenti di apt-secure possono incontrare problemi quando usano **aptitude** o **apt-get**. Per apt-get si può utilizzare **apt-get update --allow-releaseinfo-change**.

4.4.3 Accertarsi di avere spazio disponibile a sufficienza per l'aggiornamento

Prima di aggiornare il proprio sistema ci si deve accertare di avere uno spazio disponibile sufficiente sul proprio disco fisso al momento di far partire l'aggiornamento completo del sistema, come descritto in Sezione 4.4.5. Per prima cosa, poiché ogni pacchetto necessario per l'installazione prelevato dalla rete è immagazzinato in `/var/cache/apt/archives` (e nella sottodirectory `partial/`, durante lo scaricamento), ci si dovrebbe assicurare di avere spazio a sufficienza nella partizione del file system che

contiene `/var` per il temporaneo scaricamento dei pacchetti che saranno installati nel sistema. Dopo lo scaricamento sarà probabilmente necessario avere ulteriore spazio disponibile in altre partizioni del file system per poter installare sia i pacchetti aggiornati (che potrebbero contenere file binari più grossi o più dati), sia i nuovi pacchetti che saranno introdotti con l'aggiornamento. Se il sistema non ha spazio libero a sufficienza, si potrebbe finire con un aggiornamento incompleto dal quale è difficile effettuare un ripristino.

apt può mostrare informazioni dettagliate sullo spazio su disco necessario per l'installazione. È possibile visualizzare questa stima prima di eseguire effettivamente l'aggiornamento, eseguendo:

```
# apt -o APT::Get::Trivial-Only=true full-upgrade
[ ... ]
XXX aggiornati, XXX installati, XXX da rimuovere e XXX non aggiornati.
È necessario scaricare xx.xMB di archivi.
Dopo quest'operazione, verranno occupati AAAMB di spazio su disco.
```

> **NOTA**
>
> 
>
> L'esecuzione di questo comando all'inizio del processo di aggiornamento potrebbe restituire un errore, per le ragioni descritte nelle sezioni seguenti. In tal caso sarà necessario attendere finché non sarà stato eseguito l'aggiornamento minimo del sistema come descritto in Sezione 4.4.4 prima di eseguire il comando per avere una stima dello spazio necessario su disco.

Se lo spazio disponibile è insufficiente per l'aggiornamento, **apt** avverte con un messaggio come questo:

```
E: Spazio libero in /var/cache/apt/archives/ insufficiente.
```

In questo caso, accertarsi di liberare prima uno spazio sufficiente. È possibile:

- Rimuovere i pacchetti che sono stati precedentemente scaricati per l'installazione (in `/var/cache/apt/archives`). Pulire la cache dei pacchetti eseguendo **apt clean** rimuoverà tutti i file dei pacchetti scaricati in precedenza.

- Rimuovere i pacchetti dimenticati. Se si è usato **aptitude** o **apt** per installare manualmente dei pacchetti in buster, questi avranno tenuto traccia dei pacchetti installati manualmente e saranno capaci di marcare come obsoleti quei pacchetti installati solo per soddisfare delle dipendenze e che non sono più necessari se un pacchetto viene rimosso. Non marcheranno per la rimozione i pacchetti che sono stati installati manualmente dall'utente. Per rimuovere i pacchetti installati automaticamente che non sono più usati, eseguire:

  ```
  # apt autoremove
  ```

  Si può anche utilizzare **deborphan**, **debfoster** o **cruft** per trovare i pacchetti ridondanti. Non si rimuovano alla cieca i pacchetti presentati dagli strumenti, soprattutto se si usano opzioni aggressive non predefinite che possono produrre dei falsi positivi. È altamente raccomandato controllare manualmente i pacchetti suggeriti per la rimozione (ossia il loro contenuto, la loro dimensione e la descrizione) prima di rimuoverli.

- Rimuovere i pacchetti che occupano molto spazio sul disco e non sono al momento necessari (possono sempre essere reinstallati dopo l'aggiornamento). Se si ha `popularity-contest` installato, si può usare **popcon-largest-unused** per elencare i pacchetti che non si usano e che occupano più spazio. I pacchetti che occupano più spazio possono essere trovati con **dpigs** (disponibile nel pacchetto `debian-goodies`) oppure con **wajig** (eseguendo `wajig size`). Possono anche essere trovati con `aptitude`. Avviare **aptitude** in modalità a tutto terminale, selezionare Viste → Nuovo elenco unito dei pacchetti, premere **l** e inserire `~i`, premere **S** e inserire `~installsize`, a quel punto si dovrebbe ottenere un bell'elenco con cui lavorare.

- Eliminare i file di traduzioni e localizzazioni dal sistema se non sono necessari. È possibile installare il pacchetto `localepurge` e configurarlo in modo che solo poche localizzazioni selezionate vengano mantenute sul sistema. Questo ridurrà lo spazio su disco occupato da `/usr/share/locale`.
- Spostare temporaneamente su un altro sistema o rimuovere in modo permanente i log di sistema che si trovano in `/var/log`.
- Usare un `/var/cache/apt/archives` temporaneo: è possibile usare una directory di cache temporanea da un altro file system (periferiche di memorizzazione USB, dischi fissi temporanei, file system già in uso, ecc.).

> NOTA
>
> Non si usi una partizione montata via NFS, in quanto la connessione di rete potrebbe essere interrotta durante l'aggiornamento.

Per esempio, se si possiede un disco o una penna USB montato in `/media/usbkey`:

1. si rimuovano i pacchetti precedentemente scaricati per l'installazione:
   ```
   # apt clean
   ```
2. si copi la directory `/var/cache/apt/archives` nella periferica USB:
   ```
   # cp -ax /var/cache/apt/archives /media/usbkey/
   ```
3. si monti la directory della cache temporanea su quella attuale:
   ```
   # mount --bind /media/usbkey/archives /var/cache/apt/archives
   ```
4. dopo l'aggiornamento, si ripristini la directory `/var/cache/apt/archives` originale:
   ```
   # umount /var/cache/apt/archives
   ```
5. si rimuova il restante `/media/usbkey/archives`.

È possibile creare la cache temporanea su qualsiasi file system montato sul proprio sistema.

- Effettuare un aggiornamento minimo del sistema (vedere Sezione 4.4.4) oppure degli aggiornamenti parziali seguiti da un aggiornamento completo. Questo permette l'aggiornamento parziale del sistema e permette di pulire la cache dei pacchetti prima dell'aggiornamento completo.

Si noti che per rimuovere pacchetti in modo sicuro è preferibile tornare a far puntare i propri file source-list di APT a buster, come descritto in Sezione A.2.

4.4.4 Aggiornamento minimo del sistema

> IMPORTANTE
>
> Se si sta aggiornando da remoto, fare attenzione a Sezione 5.1.22.

In alcuni casi, eseguire direttamente un aggiornamento completo (come descritto più avanti) potrebbe rimuovere un gran numero di pacchetti che si potrebbe voler mantenere. È quindi raccomandato un processo di aggiornamento in due parti: prima un aggiornamento minimo che risolva questi conflitti, poi un aggiornamento completo come descritto in Sezione 4.4.5.

Per farlo eseguire:

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

Questo consentirà l'aggiornamento di quei pacchetti che possono essere aggiornati senza richiedere l'installazione o la rimozione di altri pacchetti.

L'aggiornamento minimo può essere utile anche quando non è possibile effettuare un aggiornamento completo perché sul sistema c'è poco spazio libero.

Se è installato il pacchetto `apt-listchanges`, esso mostrerà (con la sua configurazione predefinita) all'interno di un paginatore informazioni importanti sui pacchetti aggiornati dopo lo scaricamento dei pacchetti. Premere **q** dopo averle lette, per uscire dal paginatore e continuare l'aggiornamento.

4.4.5 Aggiornamento del sistema

Una volta completati i passaggi descritti in precedenza, si è pronti per continuare con la parte principale dell'aggiornamento. Si esegua:

```
# apt full-upgrade
```

Questo comando eseguirà un aggiornamento completo del sistema, installando le versioni più recenti disponibili di tutti i pacchetti e risolvendo i possibili cambiamenti di dipendenze fra i pacchetti dei diversi rilasci. Se necessario, esso installerà taluni nuovi pacchetti (normalmente nuove versioni di librerie o pacchetti rinominati) e rimuoverà i pacchetti resi obsoleti in conflitto.

In caso di aggiornamento da una serie di CD/DVD/BD, probabilmente verrà chiesto di inserire uno specifico disco in diversi momenti dell'aggiornamento. Potrebbe capitare di dover inserire più volte lo stesso disco: ciò è dovuto a pacchetti correlati tra loro che sono stati distribuiti su diversi dischi.

Nuove versioni di pacchetti attualmente installati che non possono essere aggiornati senza modificare lo stato d'installazione di un altro pacchetto saranno lasciate alla loro attuale versione (contrassegnati come «held back»;, «bloccati»). Ciò può essere risolto o utilizzando **aptitude**, per designare tali pacchetti per l'installazione, o provando con `apt install` *`pacchetto`*.

4.5 Possibili problemi durante l'aggiornamento

Nelle prossime sezioni sono descritti i problemi noti che potrebbero verificarsi durante l'aggiornamento a bullseye.

4.5.1 Dist-upgrade fallisce con l'errore «Impossibile eseguire immediatamente la configurazione»

In alcuni casi il passo **apt full-upgrade** può fallire dopo aver scaricato i pacchetti, con l'errore:

```
E: Impossibile eseguire immediatamente la configurazione su "pacchetto". Per i ↩
    dettagli vedere APT::Immediate-Configure in man 5 apt.conf.
```

Se ciò si verifica, l'esecuzione invece di **apt full-upgrade -o APT::Immediate-Configure=0** dovrebbe permettere all'aggiornamento di continuare.

Un altro possibile modo di aggirare questo problema è di aggiungere entrambe le fonti buster e bullseye ai propri file source-list di APT ed eseguire **apt update**.

4.5.2 Rimozioni attese

Il processo d'aggiornamento a bullseye potrebbe richiedere la rimozione di pacchetti dal sistema. L'elenco preciso dei pacchetti varia in base ai pacchetti installati. Queste note di rilascio forniscono un suggerimento generico riguardo le rimozioni di pacchetti, ma, nel dubbio, prima di proseguire si raccomanda di esaminare le rimozioni dei pacchetti che vengono proposte. Per maggiori informazioni sui pacchetti obsoleti in bullseye vedere Sezione 4.8.

4.5.3 Conflitti e pre-dipendenze cicliche

Talvolta è necessario abilitare l'opzione `APT::Force-LoopBreak` affinché APT possa rimuovere temporaneamente un pacchetto essenziale, a causa di un circolo «è in conflitto con»/«pre-dipende da». Di norma **apt** emette un avviso e cessa l'aggiornamento. Si può evitare questa situazione specificando l'opzione `-o APT::Force-LoopBreak=1` nella riga di comando di **apt**.

È possibile che la struttura di dipendenze di un sistema sia talmente compromessa da richiedere un intervento manuale; ciò normalmente significa l'uso di **apt** o di

```
# dpkg --remove nome_pacchetto
```

per eliminare alcuni dei pacchetti che generano il problema, o

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

In casi estremi potrebbe essere necessario forzare la re-installazione con un comando del tipo di

```
# dpkg --install /percorso/di/nome_pacchetto.deb
```

4.5.4 Conflitti tra file

Non si dovrebbero verificare conflitti tra file se si aggiorna da un sistema buster «puro», ma potrebbero verificarsi se sono stati installati backport non ufficiali. Un conflitto tra file causerà un errore simile al seguente:

```
Spacchetto <pacchetto-tizio> (da <file-del-pacchetto-tizio>) ...
dpkg: errore processando <pacchetto-tizio> (--install):
tentata sovrascrittura di '<nome-di-qualche-file>',
che si trova anche nel pacchetto <pacchetto-caio>
dpkg-deb: il sottoprocesso paste è stato terminato da un segnale (Pipe rotta)
Sono occorsi degli errori processando:
<pacchetto-tizio>
```

Si può tentare di risolvere un conflitto fra file rimuovendo forzatamente il pacchetto menzionato nell'*ultima* riga del messaggio d'errore:

```
# dpkg -r --force-depends nome_pacchetto
```

Dopo aver risolto questo problema, si dovrebbe poter riprendere l'aggiornamento ripetendo i comandi **apt** descritti in precedenza.

4.5.5 Modifiche alla configurazione

Durante l'aggiornamento verranno poste domande riguardanti la configurazione o la riconfigurazione di parecchi pacchetti. Quando viene chiesto se un qualsiasi file nella directory `/etc/init.d` o il file `/etc/manpath.config` deve essere sostituito con quello fornito dal manutentore del pacchetto, di solito è necessario rispondere affermativamente, per garantire la coerenza del sistema. Si può sempre ritornare alle versioni precedenti, dal momento che queste verranno salvate con l'estensione `.dpkg-old`.

Se non si è sicuri sul da farsi, ci si annoti il nome del pacchetto o del file e si sistemino le cose in un momento successivo. Le informazioni presentate sullo schermo durante l'aggiornamento possono essere riesaminate dopo essere state cercate nel file generato durante l'aggiornamento.

4.5.6 Cambiare la sessione sulla console

Quando si usa la console locale del sistema per fare l'aggiornamento, potrebbe accadere che durante l'aggiornamento la console sia spostata su una vista diversa e che si perda la visibilità del processo d'aggiornamento. Questo può accadere, per esempio, sui sistemi con un'interfaccia grafica quando viene riavviato il display manager.

Per recuperare la console su cui era in corso l'aggiornamento, usare Ctrl + Alt + F1, se si è nella schermata di avvio grafico, oppure usare Alt + F1 se si è in una console testuale locale, per tornare al

terminale virtuale 1. Al posto di F1 usare il tasto funzione con lo stesso numero del terminale virtuale su cui era in corso l'aggiornamento. Per scorrere i diversi terminali in modalità testuale è possibile usare Alt + Freccia sinistra o Alt + Freccia destra.

4.6 Aggiornare il kernel e i pacchetti collegati

Questa sezione spiega come aggiornare il kernel e identifica le relative potenziali problematiche. Si può o installare uno dei pacchetti `linux-image-*` forniti da Debian, oppure compilare un kernel personalizzato dai sorgenti.

Si noti che molte informazioni in questa sezione sono basate sull'assunzione che si utilizzerà uno dei kernel modulari di Debian, insieme con `initramfs-tools` e `udev`. Se si sceglie di utilizzare un kernel personalizzato che non richiede un initrd, o se si utilizza un generatore di initrd differente, alcune delle informazioni potrebbero non essere attinenti al proprio caso specifico.

4.6.1 Installazione di un metapacchetto del kernel

Quando si effettua il full-upgrade da buster a bullseye è fortemente raccomandata, se non è ancora stata fatta, l'installazione di un metapacchetto linux-image-*. Questi metapacchetti richiamano automaticamente una nuova versione del kernel durante gli aggiornamenti. si può verificare se ne è installato uno eseguendo:

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

Se non si vede alcun output, si dovrà installare manualmente un nuovo pacchetto linux-image oppure installare un metapacchetto linux-image. Per vedere un elenco dei metapacchetti linux-image disponibili eseguire:

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

Se non si è sicuri sul pacchetto da selezionare, si esegua `uname -r` e si cerchi un pacchetto con un nome simile. Ad esempio, se si vede «`4.9.0-8-amd64`» è raccomandata l'installazione di `linux-image-amd64`. Si può anche utilizzare **apt** per vedere una lunga descrizione di ciascun pacchetto che aiuti a scegliere il migliore disponibile. Ad esempio:

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

Si dovrebbe quindi utilizzare `apt install` per installarlo. Una volta che questo nuovo kernel è installato si dovrebbe riavviare alla prossima opportunità disponibile per poter godere dei benefici offerti dalla nuova versione del kernel. Tuttavia guardare Sezione 5.1.24 prima di effettuare il primo riavvio dopo l'aggiornamento.

Per i più avventurosi esiste un modo agevole per compilare il proprio kernel personalizzato su Debian. Si installino i sorgenti del kernel forniti nel pacchetto `linux-source`. Per compilare un pacchetto binario si può usare il target `deb-pkg` disponibile nel makefile dei sorgenti. Ulteriori informazioni possono essere trovate nel Debian Linux Kernel Handbook (`https://kernel-team.pages.debian.net/kernel-handbook/`), che può a sua volta essere trovato anche nel pacchetto `debian-kernel-handbook`.

Se possibile, è preferibile aggiornare il pacchetto del kernel separatamente dall'aggiornamento `full-upgrade` principale, per ridurre i rischi di trovarsi con un sistema temporaneamente non avviabile. Si noti che questo dovrebbe essere fatto soltanto dopo il processo di aggiornamento minimo descritto in Sezione 4.4.4.

4.7 Preparazione per il prossimo rilascio

Dopo l'aggiornamento ci sono molte cose che si possono fare per prepararsi per il prossimo rilascio.

- Si rimuovano i pacchetti ora obsoleti o ridondanti come descritto in Sezione 4.4.3 e Sezione 4.8. Si dovrebbe controllare quali file di configurazione questi usano e considerare l'eliminazione completa dei pacchetti per rimuovere i loro file di configurazione. Vedere anche Sezione 4.7.1.

4.7.1 Eliminare completamente i pacchetti rimossi

È generalmente consigliabile eliminare completamenti i pacchetti rimossi. Questo è particolarmente vero se i pacchetti sono stati rimossi in aggiornamenti a rilasci precedenti (es. nell'aggiornamento a buster) o se sono stati forniti da produttori esterni. In particolare è noto che i vecchi script init.d possono causare problemi.

> ATTENZIONE
>
> 
>
> L'eliminazione completa di un pacchetto in genere elimina anche i suoi file di log, perciò può essere desiderabile farne prima un backup.

Il comando seguente mostra un elenco di tutti i pacchetti rimossi che potrebbero avere dei file di configurazione rimasti nel sistema:

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

I pacchetti possono essere rimossi usando **apt purge**. Ipotizzando di volerli eliminare completamente tutti in una volta, si può usare il comando seguente:

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

Se si usa `aptitude` si possono anche usare le seguenti alternative ai comandi precedenti:

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

4.8 Pacchetti obsoleti

bullseye introduce moltissimi nuovi pacchetti, ma nel contempo ritira e manca di alcuni vecchi pacchetti che erano presenti in buster. Non viene fornito alcun percorso di aggiornamento per questi pacchetti obsoleti. Nulla impedisce di continuare a usare pacchetti obsoleti, se così si desidera, ma il progetto Debian terminerà solitamente il supporto di sicurezza per essi un anno dopo il rilascio di bullseye[5] e normalmente non fornirà altro supporto oltre a quello nel frattempo. È raccomandata la loro sostituzione con le alternative disponibili, se ve ne sono.

Vi sono molte ragioni per cui i pacchetti possono essere stati rimossi dalla distribuzione: non sono più mantenuti a monte, non vi sono più sviluppatori Debian interessati alla manutenzione dei pacchetti, le funzionalità fornite sono state superate da altri software o da una nuova versione, oppure non sono più considerati adatti per bullseye a causa di errori. In quest'ultimo caso, i pacchetti potrebbero continuare a essere presenti nella distribuzione «unstable».

Alcuni frontend per la gestione dei pacchetti forniscono modi semplici di trovare i pacchetti installati che non sono più disponibili da alcun repository noto. L'interfaccia utente testuale **aptitude** li elenca nella categoria «Pacchetti obsoleti e creati localmente» e possono essere elencati ed eliminati definitivamente dalla riga di comando usando:

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

Il Sistema di tracciamento dei bug (BTS) di Debian (`https://bugs.debian.org/`) fornisce spesso informazioni aggiuntive sul perché un determinato pacchetto è stato rimosso. Si dovrebbero visionare sia i rapporti per il pacchetto stesso, sia i rapporti archiviati dei bug per lo pseudo-pacchetto ftp.debian.org (`https://bugs.debian.org/cgi-bin/pkgreport.cgi?pkg=ftp.debian.org&archive=yes`).

Per un elenco dei pacchetto obsoleti per Bullseye fare riferimento a Sezione 5.3.1.

[5] O per tutto il tempo in cui non uscirà un altro rilascio. Tipicamente solo due rilasci stabili sono supportati contemporaneamente.

4.8.1 Pacchetti fittizi di transizione

Alcuni pacchetti da buster possono essere stati sostituiti in bullseye da pacchetti fittizi di transizione, che sono segnaposti vuoti progettati per semplificare gli aggiornamenti. Se, per esempio, un'applicazione che era precedentemente in un singolo pacchetto è stata suddivisa in diversi, può essere fornito un pacchetto di transizione con lo stesso nome del vecchio pacchetto e con le dipendenze appropriate per far sì che siano installati i nuovi. Dopo che ciò è avvenuto il pacchetto fittizio ridondante può essere rimosso senza problemi.

Le descrizioni dei pacchetti fittizi di transizione solitamente indicano il loro scopo. Tuttavia non sono uniformi; in particolare alcuni pacchetti «fittizi» sono progettati per rimanere installati allo scopo di richiamare una suite software completa o per tracciare l'attuale versione più recente di un certo programma. Si può anche trovare utile **deborphan** con le opzioni `--guess-*` (per esempio `--guess-dummy`) per identificare i pacchetti fittizi di transizione nel proprio sistema.

Capitolo 5

Problemi di cui essere al corrente per bullseye

A volte i cambiamenti introdotti da un nuovo rilascio comportano effetti collaterali che non si possono ragionevolmente evitare o che espongono errori da altre parti. In questa sezione sono documentati i problemi noti. Si leggano anche le errata corrige, la documentazione dei pacchetti interessati, le segnalazioni di errori e altre informazioni riportate in Sezione 6.1.

5.1 Aspetti specifici dell'aggiornamento a bullseye

Questa sezione tratta le voci relative all'aggiornamento da buster a bullseye.

5.1.1 Il file system XFS non supporta più l'opzione barrier/nobarrier

Il supporto per le opzioni di montaggio `barrier` e `nobarrier` è stato rimosso dal file system XFS. È raccomandato controllare se in `/etc/fstab` è presente l'una o l'altra parola chiave e rimuoverla. Le partizioni che usano tali opzioni non verranno montate con successo.

5.1.2 Struttura dell'archivio di sicurezza modificata

Per bullseye, la suite di sicurezza si chiama ora `bullseye-security` invece di *`nome-in-codice/`* e gli utenti devono adattare i loro file source-list di APT di conseguenza, quando aggiornano.

La riga per la sicurezza nella configurazione di APT dell'utente può essere del tipo:

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

Se la propria configurazione di APT include anche pinning o `APT::Default-Release`, è probabile che richieda aggiustamenti dato che il nome in codice dell'archivio di sicurezza non corrisponde più a quello dell'archivio regolare. Un esempio di riga `APT::Default-Release` funzionante per bullseye è:

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

che sfrutta la funzionalità di APT che gestisce espressioni regolari (dentro `/`).

5.1.3 Gli hash delle password usano yescrypt in modo predefinito

L'hash predefinito per le password per gli account nel sistema locale è stato cambiato (`https://tracker.debian.org/news/1226655/accepted-pam-140-3-source-into-unstable/`) da SHA-512 a yescrypt (`https://www.openwall.com/yescrypt/`) (vedere crypt(5) (`https://manpages.debian.org//bullseye/libcrypt-dev/crypt.5.html`)). Ci si aspetta che questo fornisca una sicurezza migliorata rispetto ad attacchi per indovinare le password basati su dizionario, in termini della complessità sia nello spazio che nel tempo degli attacchi.

Per sfruttare questa sicurezza migliorata, cambiare le password locali; per esempio usare il comando **passwd**.

Le vecchie password continueranno a funzionare usando l'hash per password che era stato usato per crearle, qualunque esso sia.

Yescript non è supportato da Debian 10 (buster). Di conseguenza i file password shadow (`/etc/shadow`) non possono essere copiati da un sistema bullseye in un sistema buster. Se si copiano tali file, le password che sono state cambiate nel sistema bullseye non funzioneranno nel sistema buster. In modo simile, non si può fare il copia-e-incolla degli hash di password da un sistema bullseye ad un sistema buster.

Se è richiesta la compatibilità degli hash delle password tra bullseye e buster, modificare `/etc/pam.d/common-password`. Trovare la riga simile a:

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

e sostituire `yescrypt` con `sha512`.

5.1.4 Il supporto per NSS NIS e NIS+ richiede nuovi pacchetti

Il supporto per NSS NIS e NIS + è stato spostato in pacchetti separati chiamati `libnss-nis` e `libnss-nisplus`. Purtroppo, `glibc` non può dipendere da tali pacchetti, perciò sono adesso solo raccomandati.

Nei sistemi che usano NIS o NIS + è perciò raccomandato controllare che tali pacchetti siano correttamente installati dopo l'aggiornamento.

5.1.5 Gestione di frammenti di file di configurazione in unbound

Il risolutore DNS `unbound` ha cambiato il modo in cui gestisce i frammenti di file di configurazione. Se si fa affidamento sun una direttiva `include:` per fondere diversi frammenti in una configurazione valida, si dovrebbe leggere il file NEWS (`https://sources.debian.org/src/unbound/bullseye/debian/NEWS/`).

5.1.6 Parametri di rsync resi deprecati

The `rsync` parameter `--noatime` has been renamed `--open-noatime`. The old form is no longer supported; if you are using it you should see the NEWS file (`https://sources.debian.org/src/rsync/bullseye/debian/rsync.NEWS/`). Transfer processes between systems running different Debian releases may require the buster side to be upgraded to a version of `rsync` from the backports (`https://backports.debian.org/`) repository. The version of `rsync` in the initial release of bullseye also deprecated `--copy-devices` in favor of `--write-devices`, but version 3.2.3-4 + deb11u1 (included in bullseye point release 11.1) reverts this deprecation and supports both options.

5.1.7 Gestione degli addon di Vim

I moduli aggiuntivi per `vim` storicamente forniti da `vim-scripts` sono ora gestiti attraverso la funzionalità nativa «package» di Vim, invece che da `vim-addon-manager`. Gli utenti di Vim dovrebbero prepararsi prima dell'aggiornamento seguendo le istruzioni nel file NEWS (`https://sources.debian.org/src/vim-scripts/bullseye/debian/NEWS/`).

5.1.8 OpenStack e cgroups v1

OpenStack Victoria (rilasciato in bullseye) richiede cgroup v1 per QoS dei device a blocchi. A partire da bullseye passa anche ad usare cgroupv2 in modo predefinito (vedere Sezione 2.2.4), l'albero sysfs in `/sys/fs/cgroup` non include funzionalità cgroup v1 come `/sys/fs/cgroup/blkio`, e come risultato **cgcreate -g blkio:foo** fallisce. Per i nodi OpenStack con in esecuzione `nova-compute` o `cinder-volume` è fortemente raccomandato aggiungere i parametri `systemd.unified_cgroup_hierarchy=false` e `systemd.legacy_systemd_cgroup_controller=false` alla riga di comando del kernel per scavalcare i valori predefiniti e ripristinare la vecchia gerarchia di cgroup.

5.1.9 File di politica dell'API OpenStack

Seguendo le raccomandazioni degli autori originali, OpenStack Victoria nel rilascio bullseye passa per l'API OpenStack all'uso del nuovo formato YAML. Come risultato, la maggior parte dei servizi OpenStack, inclusi Nova, Glance e Keystone appaiono non funzionanti con tutte le politiche per API scritte esplicitamente nei file `policy.json`. I pacchetti, perciò, vengono ora forniti con una directory `/etc/PROJECT/policy.d` contenente un file `00_default_policy.yaml` con tutte le politiche commentate in modo predefinito.

Per evitare che il vecchio file `policy.json` rimanga attivo, i pacchetti OpenStack di Debian ora lo rinominano in `disabled.policy.json.old`. In alcuni casi, quando non è stato possibile fare nulla di meglio prima del rilascio, `policy.json` viene semplicemente eliminato. Perciò, prima di aggiornare, è fortemente consigliato di fare il backup dei file `policy.json` delle proprie installazioni.

Ulteriori dettagli sono disponibili nella documentazione originale (`https://governance.openstack.org/tc/goals/selected/wallaby/migrate-policy-format-from-json-to-yaml.html`).

5.1.10 sendmail non attivo durante l'aggiornamento

A differenza dei normali aggiornamenti di `sendmail`, durante l'aggiornamento da buster a bullseye il servizio sendmail viene fermato, determinando una mancanza di servizio più lunga del consueto. Per un suggerimento generico su come ridurre il tempo di inattività, vedere Sezione 4.1.3.

5.1.11 FUSE 3

Alcuni pacchetti, inclusi `gvfs-fuse`, `kio-fuse` e `sshfs` sono passati a FUSE 3. Durante gli aggiornamenti ciò causerà l'installazione di `fuse3` e la rimozione di `fuse`.

In alcune circostanze eccezionali, ad esempio quando si effettua l'aggiornamento eseguendo solamente **apt-get dist-upgrade** invece dei passaggi di aggiornamento raccomandati da Capitolo 4, i pacchetti che dipendono da `fuse3` possono essere mantenuti fermi durante l'aggiornamento. Eseguire nuovamente i passaggi descritti in Sezione 4.4.5 con `apt` di bullseye o aggiornarli manualmente risolverà la situazione.

5.1.12 File delle opzioni di GnuPG

A partire dalla versione 2.2.27-1, la configurazione del singolo utente della suite `GnuPG` è stata completamente spostata in `~/.gnupg/gpg.conf` e `~/.gnupg/options` non è più utilizzato. Rinominare il file se necessario o spostare i suoi contenuti nella nuova posizione.

5.1.13 Linux abilita gli spazi dei nomi utente in modo predefinito

A partire da `Linux` 5.10, viene permesso, in modo predefinito, a tutti gli utenti di creare spazi dei nomi utente. Ciò permette a programmi come browser web e gestori di contenuti di creare sandbox più ristrette per codice non fidato o meno fidato, senza la necessità di essere eseguito come root o di usare uno strumento ausiliario setuid-root.

Il comportamento predefinito della Debian precedente era di restringere questa funzionalità ai processi in esecuzione come root, perché esponeva più problemi di sicurezza nel kernel. Tuttavia, ora che l'implementazione di questa funzionalità è maturata, c'è la convinzione che i benefici di sicurezza che essa fornisce superino i rischi connessi alla sua abilitazione.

Se si preferisce mantenere ristretta funzionalità, impostare sysctl:

```
user.max_user_namespaces = 0
```

Notare che varie funzionalità di desktop e contenitori non funzioneranno con questa restrizione, inclusi browser web, `WebKitGTK`, `Flatpak` e miniature di `GNOME`.

L'impostazione sysctl `kernel.unprivileged_userns_clone=0` specifica di Debian ha un effetto simile, ma è deprecata.

5.1.14 Linux disabilita chiamate non privilegiate a bpf() in modo predefinito

A partire da `Linux` 5.10, Debian disabilita chiamate non privilegiate a bpf() in modo predefinito. Tuttavia, un amministratore può sempre cambiare, se necessario, questa impostazione in un secondo momento scrivendo 0 o 1 nel sysctl `kernel.unprivileged_bpf_disabled`.

Se si preferisce mantenere abilitate le chiamate non privilegiate a bpf(), impostare sysctl:

```
kernel.unprivileged_bpf_disabled = 0
```

Per informazioni sulla modifica del comportamento predefinito in Debian vedere il bug 990411 (`https://bugs.debian.org/990411`) con la richiesta di modifica.

5.1.15 redmine mancante in bullseye

Il pacchetto `redmine` non viene fornito in bullseye, dato che era troppo tardi per migrare dalla vecchia versione di `rails`, che è alla fine del supporto a monte (ricevendo solamente le soluzioni a gravi bug di sicurezza), alla versione che è in bullseye. I manutentori di `Ruby Extras` stanno seguendo da vicino lo sviluppo a monte e rilasceranno una versione attraverso backports (`https://backports.debian.org/`) non appena verrà rilasciata e avranno pacchetti funzionanti. Se non si può aspettare che ciò avvenga prima di aggiornare, si può usare una VM o un contenitore con in esecuzione buster per isolare questa specifica applicazione.

5.1.16 Exim 4.94

Considerare la versione di Exim in bullseye come un aggiornamento *principale* di Exim. Introduce il concetto di dati contaminati ("tainted") letti da fonti non fidate, come ad esempio l'autore o il destinatario di un messaggio. Questi dati (ad esempio `$local_part` o `$domain`) non possono essere usati, tra le altre cose, come nomi di file o directory o nomi di comandi.

Questo rende *non funzionanti* configurazioni che non vengono aggiornate di conseguenza. Anche i vecchi file di configurazione di Exim in Debian non funzioneranno se non modificati; la nuova configurazione deve essere installata con le modifiche locali riunite in essa.

Esempi tipici non funzionanti includono:

- Consegna a `/var/mail/$local_part`. Usare `$local_part_data` in combinazione con `check_local_user`.
- Usare

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

  invece di

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

  per un file alias per domini virtuali.

La strategia di base per affrontare questa modifica è quella di usare il risultato di una ricerca con lookup in una successiva elaborazione invece del valore originale (fornito da remoto).

Per facilitare l'aggiornamento esiste una nuova opzione per configurazione principale per abbassare temporaneamente gli errori relativi a dati "tainted" ad avvertimenti, permettendo alla vecchia configurazione di funzionare con il nuovo Exim. Per utilizzare questa funzionalità aggiungere

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

alla configurazione di Exim (ad esempio a `/etc/exim4/exim4.conf.localmacros`) *prima* dell'aggiornamento e controllare nel file di log la presenza di avvertimenti legati a dati "tainted". Questo è un aggiramento temporaneo del problema che è già contrassegnato, al momento dell'introduzione, per la rimozione.

5.1.17 Il rilevamento di device SCSI non è deterministico

A causa di cambiamenti nel kernel Linux, il rilevamento di device SCSI non è più deterministico. Questo può essere un problema per le installazioni che si affidano all'ordine di rilevamento dei dischi. In questo messaggio nella mailing-list (`https://lore.kernel.org/lkml/59eedd28-25d4-7899-7c3c-89fe7fdd4b4acm.org/`) sono suggerite due possibili alternative che usano i collegamenti in `/dev/disk/by-path` o una regola `udev`.

5.1.18 rdiff-backup richiede aggiornamento in blocco di server e client

Il protocollo di rete delle versioni 1 e 2 di `rdiff-backup` sono incompatibili. Ciò significa che si deve eseguire la stessa versione (1 o 2) di `rdiff-backup` localmente e in remoto. Dato che buster fornisce la versione 1.2.8 e bullseye fornisce la versione 2.0.5, l'aggiornamento da buster a bullseye del solo sistema locale o del solo sistema remoto renderà non funzionante l'esecuzione di `rdiff-backup` tra i due.

La versione 2.0.5 di `rdiff-backup` è disponibile nell'archivio buster-backports archive, vedere backports (`https://backports.debian.org/`).

5.1.19 Problemi con microcodice delle CPU Intel

Il pacchetto `intel-microcode` attualmente in bullseye e buster-security (see DSA-4934-1 (`https://www.debian.org/security/2021/dsa-4934`)) contiene due bug importanti. Per alcune CPU CoffeeLake questo aggiornamento può rendere non funzionanti interfacce di rete (`https://github.com/intel/Intel-Linux-Processor-Microcode-Data-Files/issues/56`) che usano `firmware-iwlwifi` e, per alcune CPU Skylake R0/D0 su sistemi che usano un firmware/BIOS molto obsoleto, il sistema può bloccarsi all'avvio (`https://github.com/intel/Intel-Linux-Processor-Microcode-Data-Files/issues/31`).

Se si è rimandato l'aggiornamento da DSA-4934-1 a causa di questi problemi, o non si ha l'archivio di sicurezza abilitato, tenere a mente che aggiornare al pacchetto `intel-microcode` in bullseye può far sì che il sistema si blocchi all'avvio o può rendere non funzionante iwlwifi. In tal caso, si può ripristinare la situazione disabilitando il caricamento del microcodice all'avvio; vedere le istruzioni nel DSA, che sono anche nel file `README.Debian` di `intel-microcode`.

5.1.20 Gli aggiornamenti che coinvolgono libgc1c2 necessitano due esecuzioni

I pacchetti che dipendono da `libgc1c2` in buster (es. `guile-2.2-libs`) possono essere mantenuti alla versione precedente durante la prima esecuzione di un aggiornamento completo a bullseye. Fare un secondo aggiornamento solitamente risolve il problema. Le informazioni sulle basi del problema possono essere trovate nel bug n. 988963 (`https://bugs.debian.org/988963`).

5.1.21 fail2ban non può inviare email usando mail da bsd-mailx

Il pacchetto `fail2ban` può essere configurato per inviare notifiche via email. Lo fa usando **mail** che è fornito in Debian da diversi pacchetti. Un aggiornamento di sicurezza (necessario sui sistemi che usano **mail** da `mailutils`) proprio prima del rilascio di bullseye ha reso non funzionante questa funzionalità per i sistemi che hanno **mail** fornito da `bsd-mailx`. Gli utenti con `fail2ban` in combinazione con `bsd-mailx` che desiderano che `fail2ban` invii email devono passare ad un diverso fornitore di **mail** oppure rimuovere manualmente l'applicazione del commit a monte (`https://github.com/fail2ban/fail2ban/commit/410a6ce5c80dd981c22752da034f2529b5eee844`) (che ha inserito la stringa "`-E 'set escape'`" in diversi punti in `/etc/fail2ban/action.d/`).

5.1.22 Nessuna nuova connessione SSH possibile durante l'aggiornamento

Sebbene le connessioni SSH (Secure SHell) esistenti dovrebbero continuare a funzionare come di consueto durante l'aggiornamento, a causa di circostanze sfortunate il periodo in cui non è possibile stabilire nuove connessioni SSH è più lungo del solito. Se l'aggiornamento viene fatto attraverso una connessione SSH che può venire interrotta, è raccomandato aggiornare `openssh-server` prima di aggiornare il sistema completo.

5.1.23 L'aggiornamento di Open vSwitch richiede la modifica di interfaces(5)

L'aggiornamento di `openvswitch` può non riuscire a recuperare i bridge dopo l'avvio. Per aggirare il problema si deve:

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

Per maggiori informazioni vedere il bug n.989720 (`https://bugs.debian.org/989720`).

5.1.24 Cose da fare dopo l'aggiornamento prima di riavviare

Quando `apt full-upgrade` ha terminato, l'aggiornamento è «formalmente» completo. Per l'aggiornamento a bullseye non ci sono azioni speciali necessarie prima di effettuare un riavvio.

5.2 Cosa non limitate al processo di aggiornamento

5.2.1 Limitazione nel supporto per la sicurezza

Ci sono alcuni pacchetti per i quali Debian non può garantire di fornire i backport minimi per ragioni di sicurezza. Questi verranno trattati nelle sottosezioni che seguono.

NOTA

Il pacchetto `debian-security-support` aiuta a tenere traccia dello stato del supporto di sicurezza per i pacchetti installati.

5.2.1.1 Stato della sicurezza dei browser web e dei loro motori di rendering

Debian 11 contiene diversi motori per browser che sono affetti da varie vulnerabilità di sicurezza. L'alto tasso di vulnerabilità e la parziale mancanza di supporto a lungo termine da parte degli autori originali complica l'attività di supporto di questi browser e motori tramite il backport delle correzioni di sicurezza alle versioni precedenti. Inoltre la dipendenza reciproca delle librerie rende estremamente difficile aggiornare a una nuova versione a monte. Perciò, in bullseye sono presenti browser basati ad esempio sui motori webkit e khtml[1], ma non sono coperti dal supporto di sicurezza. Non si dovrebbe usare questi browser con siti web non fidati. I motori webkit2gtk e wpewebkit sono coperti dal supporto di sicurezza.

Per un browser web di uso generico vengono raccomandati Firefox o Chromium. Verranno mantenuti aggiornati ricompilando gli attuali rilasci ESR per stable. La stessa strategia verrà seguita per Thunderbird.

5.2.1.2 OpenJDK 17

Debian bullseye viene fornita con una versione di anteprima di `OpenJDK 17` (la nuova versione pianificata di `OpenJDK LTS` dopo `OpenJDK 11`), per evitare il piuttosto laborioso lavoro di bootstrap. Il piano è quello che `OpenJDK 17` riceva un aggiornamento in bullseye al rilascio finale a monte annunciato per ottobre 2021, seguito dagli aggiornamenti di sicurezza nel modo migliore possibile in base alle risorse umane, ma gli utenti non si devono attendere aggiornamenti per ogni aggiornamento di sicurezza trimestrale a monte.

[1] Questi motori vengono forniti in svariati diversi pacchetti sorgenti e le preoccupazioni valgono per tutti i pacchetti che li forniscono. La preoccupazione si estende anche ai motori di rendering web qui non menzionati esplicitamente, con l'eccezione di webkit2gtk e il nuovo wpewebkit.

5.2.1.3 Pacchetti basati su Go

L'infrastruttura Debian attualmente ha problemi con la ricompilazione di pacchetti del tipo che usa sistematicamente link statici. Prima di buster questo non era in pratica un problema, ma con il crescere dell'ecosistema Go ciò significa che i pacchetti basati su Go saranno coperti da un supporto di sicurezza limitato fino a che l'infrastruttura non sarà migliorata per poter lavorare con essi in modo mantenibile.

Se sono necessari aggiornamenti per le librerie di sviluppo di Go, questi possono solamente passare attraverso i regolari rilasci minori, che possono essere lenti ad arrivare.

5.2.2 Accesso all'applicazione delle Impostazioni di GNOME senza mouse

Senza un dispositivo puntatore non esiste un modo diretto per cambiare le impostazioni nell'applicazione Impostazioni di GNOME fornita da `gnome-control-center`. Per aggirare il problema si può navigare dalla barra laterale ai contenuti principali usando **freccia a destra** due volte. Per ritornare alla barra laterale si può avviare una ricerca con Ctrl + F, digitare qualcosa, poi premere **Esc** per annullare la ricerca. Ora si possono usare **Freccia in su** e **Freccia in giù** per navigare nella barra laterale. Non è possibile selezionare i risultati di una ricerca con la tastiera.

5.2.3 L'opzione di avvio `rescue` è inutilizzabile senza la password di root

Con l'implementazione di `sulogin`, usato a partire da buster, l'avvio con l'opzione `rescue` richiede sempre la password di root. Se non ne è stata impostata una, ciò rende di fatto la modalità di ripristino inutilizzabile. È tuttavia ancora possibile avviare usando il parametro `init=/sbin/sulogin --force` del kernel.

Per configurare systemd in modo che faccia l'equivalente ogni volta che avvia in modalità ripristino (nota anche come "single mode", vedere systemd(1) (`https://manpages.debian.org//bullseye/systemd/systemd.1.html`)), eseguire **sudo systemctl edit rescue.service** e creare un file contenente solamente:

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

Potrebbe anche (o invece) essere utile farlo per l'unità `emergency.service`, che è avviata *automaticamente* nel caso di alcuni errori (vedere systemd.special(7) (`https://manpages.debian.org//bullseye/systemd/systemd.special.7.html`)) o se viene aggiunto `emergency` alla riga di comando del kernel (ad esempio se il sistema non può essere ripristinato usando la modalità di ripristino).

Per informazioni a riguardo e per una discussione sulle implicazioni in termini di sicurezza vedere #802211 (`https://bugs.debian.org//802211`).

5.2.4 32-bit Xen PV guests are not supported

The Linux kernel (from version 5.9) no longer supports 32-bit `xen` virtual machines using PV mode (`https://wiki.xenproject.org/wiki/Virtualization_Spectrum`). Such virtual machines need to be converted to the 64-bit PC architecture.

You can check which mode a Xen guest is running (inside the virtual machine):

```
$ cat /sys/hypervisor/guest_type
PV
```

Virtual machines that return, for example, `PVH` or `HVM` are not affected.

5.3 Obsolescenze e deprecazioni

5.3.1 Pacchetti obsoleti degni di nota

Quello che segue è un elenco di pacchetti obsoleti noti e degni di nota (vedere Sezione 4.8 per una descrizione).

L'elenco dei pacchetti obsoleti comprende:

- Il pacchetto `lilo` è stato rimosso da bullseye. Il successore di lilo come boot loader è `grub2`.

- La versione 3 della suite del gestore di mailing-list Mailman è l'unica versione disponibile di Mailman in questo rilascio. Mailman è stato diviso in vari componenti; la parte principale è disponibile nel pacchetto `mailman3` e la suite completa può essere ottenuta tramite il metapacchetto `mailman3-full`.

  La versione sorpassata 2.1 di Mailman non è più disponibile (una volta era il pacchetto `mailman`). Tale ramo dipende da Python 2 che non è più disponibile in Debian.

  Per le istruzioni sull'aggiornamento vedere la documentazione per migrazione del progetto. (`https://docs.mailman3.org/en/latest/migration.html`)

- Il kernel Linux non fornisce più il supporto per `isdn4linux` (i4l). Di conseguenza, i relativi pacchetti in spazio utente `isdnutils`, `isdnactivecards`, `drdsl` e `ibod` sono stati rimossi dagli archivi.

- Le librerie deprecate libappindicator non sono più fornite. Come risultato, i pacchetti relativi `libappindicator1`, `libappindicator3-1` e `libappindicator-dev` non sono più disponibili. Ci si aspetta che ciò causi errori di dipendenze per software di terze parti che dipende ancora da libappindicator per fornire la gestione del vassoio di sistema e degli indicatori.

  Debian usa `libayatana-appindicator` come successore di libappindicator. Per le basi tecniche vedere questo annuncio (`https://lists.debian.org/debian-devel/2018/03/msg00506.html`).

- Debian non fornisce più `chef`. Se si usa Chef per la gestione della configurazione, il percorso di aggiornamento migliore è probabilmente quello di passare ad usare i pacchetti forniti da Chef Inc (`https://www.chef.io/`).

  Per informazioni su ciò che è alla base della rimozione vedere la richiesta di rimozione (`https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=963750`).

- Python 2 ha già passato la sua fine vita e non riceverà aggiornamenti di sicurezza. Non è supportato per l'esecuzione di applicazioni e i pacchetti che si basano su di esso sono stati passati a Python 3 o rimossi. Tuttavia, Debian bullseye include ancora una versione di Python 2.7, oltre ad un limitato numero di strumenti di compilazione per Python 2, come `python-setuptools`. Questi sono presenti solo perché sono richiesti da alcuni processi di compilazione di applicazioni che non sono ancora state convertite a Python 3.

- Il pacchetto `aufs-dkms` non fa parte di bullseye. La maggior parte degli utenti di `aufs-dkms` dovrebbe poter passare a `overlayfs`, che fornisce funzionalità simili con il supporto del kernel. Tuttavia è possibile avere un'installazione Debian su un file system che non è compatibile con `overlayfs`, ad esempio. `xfs` senza `d_type`. Viene suggerito agli utenti di `aufs-dkms` di migrare via da `aufs-dkms` prima dall'aggiornamento a bullseye.

- Il gestore delle connessioni di rete `wicd` non sarà più disponibile dopo l'aggiornamento perciò, per evitare il pericolo di perdere la connettività, viene raccomandato agli utenti di passare prima dell'aggiornamento ad un'alternativa come `network-manager` o `connman`.

5.3.2 Componenti deprecati per bullseye

Con il prossimo rilascio di Debian 12 (nome in codice bookworm) alcune funzionalità diventeranno deprecate. Gli utenti dovranno migrare ad altre alternative per evitare problemi nell'aggiornamento a Debian 12.

Ciò include le seguenti funzionalità:

- Le motivazioni storiche per la disposizione del file system con le directory `/bin`, `/sbin` e `/lib` separate dalle loro equivalenti in `/usr` non sono al giorno d'oggi più valide; vedere la sintesi di Freedesktop.org (`https://www.freedesktop.org/wiki/Software/systemd/TheCaseForTheUsrMerge`). Debian bullseye sarà l'ultimo rilascio Debian a gestire la disposizione con usr non unificate; per i sistemi con una disposizione vecchia che sono stati aggiornati senza una reinstallazione, esiste il pacchetto `usrmerge` per fare la conversione, se la si desidera.

- bullseye è l'ultimo rilascio Debian a fornire **apt-key**. Le chiavi dovrebbero essere invece gestite mettendo i file in `/etc/apt/trusted.gpg.d`, in formato binario come creato da **gpg --export** con un'estensione `.gpg`, o con armor ASCII con un'estensione `.asc`.

  È pianificato un rimpiazzo di **apt-key list** per ispezionare manualmente il portachiavi, ma i lavori non sono ancora iniziati.

- I backend per database `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`) vengono ritirati e non saranno inclusi in Debian 12. I database LDAP che usano i backend `bdb` o `hdb` dovrebbero migrare al backend slapd-mdb(5) (`https://manpages.debian.org//bullseye/slapd/slapd-mdb.5.html`).

  Inoltre i backend slapd-perl(5) (`https://manpages.debian.org//bullseye/slapd/slapd-perl.5.html`) and slapd-sql(5) (`https://manpages.debian.org//bullseye/slapd/slapd-sql.5.html`) sono deprecati e potrebbero essere rimossi in un rilascio futuro.

  Il Progetto OpenLDAP non supporta backend ritirati o deprecati. Il supporto per questi backend in Debian 11 non è garantito ma è al meglio dello sforzo possibile.

5.4 Bug importanti conosciuti

Sebbene Debian venga rilasciata quando è pronta, ciò sfortunatamente non significa che non vi siano bug noti. Come parte del processo di rilascio tutti i bug di gravità seria o superiore sono tracciati attivamente dal Team di Rilascio, perciò una panoramica di tali bug (`https://bugs.debian.org/cgi-bin/pkgreport.cgi?users=release.debian.org@packages.debian.org;tag=bullseye-can-defer`) che sono stati etichettati come da ignorare nell'ultima parte del rilascio di bullseye può essere trovata nel Sistema di tracciamento dei bug di (BTS) (`https://bugs.debian.org/`). Al momento del rilascio, bullseye era affetta dai seguenti bug degni di nota:

Numero di bug	Pacchetto (sorgente o binario)	Descrizione
922981 (`https://bugs.debian.org/922981`)	`ca-certificates-java`	ca-certificates-java: /etc/ca-certificates/update.d/jks-keystore non aggiorna /etc/ssl/certs/java/cacerts
990026 (`https://bugs.debian.org/990026`)	`cron`	cron: charset ridotto in MAILTO causa malfunzionamento
991081 (`https://bugs.debian.org/991081`)	`gir1.2-diodon-1.0`	gir1.2-diodon-1.0 ha dipendenze mancanti
990318 (`https://bugs.debian.org/990318`)	`python-pkg-resources`	python-pkg-resources: aggiungere "Breaks" verso i pacchetti Python senza versione
991449 (`https://bugs.debian.org/991449`)	`fail2ban`	la soluzione per CVE-2021-32749 rende non funzionanti i sistemi con posta da bsd-mailx
990708 (`https://bugs.debian.org/990708`)	`mariadb-server-10.5,galera-4`	mariadb-server-10.5: problemi di aggiornamento a causa del passaggio galera-3 -> galera-4
980429 (`https://bugs.debian.org/980429`)	`src:gcc-10`	g++-10: segmentation fault spurio in c++17 mode in append_to_statement_list_1 (tree-iterator.c:65)
980609 (`https://bugs.debian.org/980609`)	`src:gcc-10`	missing i386-cpuinfo.h
984574 (`https://bugs.debian.org/984574`)	`gcc-10-base`	gcc-10-base: aggiungere "Breaks: gcc-8-base (<< 8.4)"

Numero di bug	Pacchetto (sorgente o binario)	Descrizione
984931 (https://bugs.debian.org/984931)	git-el	git-el,elpa-magit: fails to install: /usr/lib/emacsen-common/packages/install/git emacs failed at /usr/lib/emacsen-common/lib.pl line 19, <TSORT> line 7.
987264 (https://bugs.debian.org/987264)	git-el	git-el: fallisce l'installazione con xemacs21
991082 (https://bugs.debian.org/991082)	gir1.2-gtd-1.0	gir1.2-gtd-1.0 ha dipendenze vuote
948739 (https://bugs.debian.org/948739)	gparted	gparted non dovrebbe mascherare unità .mount
984714 (https://bugs.debian.org/984714)	gparted	gparted dovrebbe suggerire exfatprogs e fare il backport del commit che respinge exfat-utils
968368 (https://bugs.debian.org/968368)	ifenslave	ifenslave: opzione bond-master fallisce l'aggiunta di interfaccia a bond
990428 (https://bugs.debian.org/990428)	ifenslave	ifenslave: il bonding non funziona in bullseye (usando bond-slaves config)
991113 (https://bugs.debian.org/991113)	libpam-chroot	libpam-chroot installa pam_chroot.so nella directory sbagliata
989545 (https://bugs.debian.org/989545)	src:llvm-toolchain-11	libgl1-mesa-dri: si_texture.c:1727 si_texture_transfer_map - fallisce la creazione di texture temporanea per tenere copia "untiled"
982459 (https://bugs.debian.org/982459)	mdadm	mdadm --esame in chroot senza /proc,/dev,/sys montati corrompe il file system dell'host
981054 (https://bugs.debian.org/981054)	openipmi	openipmi: dipendenza da kmod mancante
948318 (https://bugs.debian.org/948318)	openssh-server	openssh-server: non riesce a riavviare sshd restart dopo l'aggiornamento alla versione 8.1p1-2
991151 (https://bugs.debian.org/991151)	procps	procps: abbandonata l'opzione reload dallo script init, rendendo malfunzionante corekeeper
989103 (https://bugs.debian.org/989103)	pulseaudio	pulseaudio ha una regressione sulla configurazione control=Wave
984580 (https://bugs.debian.org/984580)	libpython3.9-dev	libpython3.9-dev: dipendenza da zlib1g-dev mancante
990417 (https://bugs.debian.org/990417)	src:qemu	openjdk-11-jre-headless: l'esecuzione di java in qemu s390 causa un SIGILL a C [linux-vdso64.so.1+0x6f8] __kernel_getcpu+0x8

Numero di bug	Pacchetto (sorgente o binario)	Descrizione
859926 (https://bugs.debian.org/859926)	speech-dispatcher	non funziona con pulse-audio come output quando avviato da speechd-up dal sistema init
932501 (https://bugs.debian.org/932501)	src:squid-deb-proxy	squid-deb-proxy: il demone non si avvia perché il file conf non è permesso da apparmor
991588 (https://bugs.debian.org/991588)	tpm2-abrmd	tpm2-abrmd non dovrebbe usare Requires=systemd-udev-settle.service nella sua unità
991939 (https://bugs.debian.org/991939)	libjs-bootstrap4	libjs-bootstrap4: collegamenti simbolici interrotti: /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 elimina file non correlati al di fuori dei sorgenti del pacchetto
988477 (https://bugs.debian.org/988477)	src:xen	xen-hypervisor-4.14-amd64: xen dmesg mostra (XEN) AMD-Vi: IO_PAGE_FAULT su dispositivo sata pci
991788 (https://bugs.debian.org/991788)	xfce4-settings	xfce4-settings: schermo nero dopo sospensione quando il coperchio del laptop viene chiuso e riaperto

Capitolo 6

Maggiori informazioni su Debian

6.1 Ulteriori letture

Oltre alle presenti note di rilascio e alla guida all'installazione, ulteriore documentazione su Debian è disponibile presso il Progetto di Documentazione di Debian (DDP - Debian Documentation Project), il cui scopo è creare documentazione di alta qualità per gli utenti e gli sviluppatori di Debian, quale la Debian Reference, la guida per i nuovi manutentori Debian, le FAQ Debian e molti altri documenti. Per dettagli completi sulle risorse disponibili si consulti il sito della documentazione Debian (`https://www.debian.org/doc/`) e il Wiki Debian (`https://wiki.debian.org/`).

La documentazione per i singoli pacchetti viene installata in `/usr/share/doc/`*`pacchetto`*. Questa potrebbe includere anche informazioni sul copyright, dettagli specifici inerenti Debian e ogni altra documentazione dell'autore.

6.2 Ottenere aiuto

Ci sono molte fonti disponibili per l'aiuto, le informazioni e il supporto agli utenti di Debian, ma queste dovrebbero essere prese in considerazione solo dopo aver cercato il problema nella documentazione disponibile. Questa sezione fornisce una breve panoramica delle risorse che potrebbero essere d'aiuto ai nuovi utenti di Debian.

6.2.1 Liste di messaggi

Le liste di messaggi di maggior interesse per gli utenti di Debian sono debian-user (in inglese), debian-italian (in italiano) e le liste debian-user-*`lingua`* (per le altre lingue). Per informazioni su queste liste e dettagli sulle modalità di sottoscrizione si veda `https://lists.debian.org/`. Si raccomanda di cercare la risposta alla propria domanda negli archivi prima di inviarla e di osservare la «netiquette» standard delle liste.

6.2.2 Internet Relay Chat

Debian ha un canale IRC dedicato al supporto e all'aiuto agli utenti Debian, che si trova sulla rete IRC OFTC. Per accedere a tale canale si indirizzi il proprio client IRC preferito su irc.debian.org e si acceda a `#debian`. Il canale italiano di supporto è sulla rete IRC OFTC, `#debian-it`.

Si prega di seguire le linee guida del canale, nel pieno rispetto degli altri utenti. Queste sono disponibili nel wiki di Debian (`https://wiki.debian.org/DebianIRC`).

Per maggiori informazioni su OFTC si visiti il sito web (`http://www.oftc.net/`).

6.3 Segnalare i bug

Viene fatto ogni sforzo per rendere Debian un sistema operativo di alta qualità, ma questo non significa che i pacchetti forniti siano totalmente esenti da problemi. Coerentemente con la filosofia dello «sviluppo aperto» di Debian e come servizio per gli utenti forniamo sul sistema di tracciamento dei bug

(BTS, Bug Tracking System) tutte le informazioni disponibili sugli errori scoperti. Il BTS è consultabile all'indirizzo https://bugs.debian.org/.

Se si trova un errore nella distribuzione o in un software pacchettizzato che ne fa parte si è pregati di segnalarlo, in modo che possa essere opportunamente risolto per i rilasci futuri. Per la segnalazione degli errori è richiesto un indirizzo di posta elettronica valido, per poter tenere traccia degli errori e in modo che gli sviluppatori possano mettersi in contatto con gli autori delle segnalazioni qualora fossero necessarie maggiori informazioni.

Si può segnalare un errore utilizzando il programma **reportbug** o manualmente utilizzando la posta elettronica. Si possono ottenere maggiori informazioni sul sistema di tracciamento dei bug e su come utilizzarlo leggendo la documentazione di riferimento (disponibile in /usr/share/doc/debian, se si ha installato doc-debian) o in linea presso il Bug Tracking System (https://bugs.debian.org/).

6.4 Contribuire a Debian

Non è necessario essere degli esperti per contribuire a Debian. Assistendo gli utenti con i problemi che espongono sulle varie liste di supporto per gli utenti (https://lists.debian.org/) si fornisce un contributo alla comunità. Identificare (e anche risolvere) problemi relativi allo sviluppo della distribuzione tramite la partecipazione alle liste per lo sviluppo (https://lists.debian.org/) è un'altra attività estremamente utile. Per mantenere l'alta qualità della distribuzione Debian si possono segnalare errori (https://bugs.debian.org/), in modo da aiutare gli sviluppatori a trovarli e a correggerli. Lo strumento how-can-i-help aiuta a trovare dei bug segnalati adatti su cui lavorare. Se si è portati per la scrittura si potrebbe voler fornire più attivamente un contributo aiutando a scrivere la documentazione (https://www.debian.org/doc/vcs) o a tradurre (https://www.debian.org/international/) nella propria lingua la documentazione esistente.

Se si ha più tempo da dedicare, si può provvedere alla gestione di una parte della raccolta di software libero contenuta in Debian. È particolarmente utile che delle persone adottino o mantengano elementi che altre persone hanno richiesto di includere in Debian. I dettagli a tal proposito si trovano nel database Work Needing and Prospective Packages (https://www.debian.org/devel/wnpp/). Se si ha un interesse verso qualche area specifica, si potrebbe trovare piacevole fornire un contributo a qualcuno fra i sottoprogetti di Debian (https://www.debian.org/devel/#projects), che comprendono port verso architetture particolari e, fra i molti altri, Debian Pure Blends (https://wiki.debian.org/DebianPureBlends) per specifici gruppi di utenti.

In ogni caso, se si sta lavorando all'interno della comunità del software libero in un qualunque ambito come utente, programmatore, scrittore o traduttore, si sta già dando un contributo alla causa del software libero. Contribuire è gratificante e divertente e, oltre a permettere di incontrare nuove persone, dà quella certa sensazione interiore di benessere.

Capitolo 7

Glossario

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

Appendice A

Gestire il proprio sistema buster prima dell'avanzamento

Questa appendice contiene informazioni su come accertarsi di poter aggiornare o installare i pacchetti di buster prima di aggiornare a bullseye. Questo dovrebbe essere necessario solo in casi particolari.

A.1 Aggiornare il proprio sistema buster

In linea di principio non vi è alcuna differenza rispetto a qualsiasi altro aggiornamento effettuato in precedenza per buster. L'unica differenza è che dapprima sarà necessario accertarsi che il proprio elenco dei pacchetti contenga ancora i riferimenti a buster come illustrato in Sezione A.2.

Se si aggiorna il proprio sistema utilizzando un mirror Debian, esso sarà aggiornato automaticamente all'ultimo point release (rilascio minore) di buster.

A.2 Controllare i propri file source-list per APT

Se qualsiasi riga nei propri file source-list di APT (vedere sources.list(5) (`https://manpages.debian.org//bullseye/apt/sources.list.5.html`)) contiene riferimenti a «`stable`», in effetti sta già puntando a bullseye. Ciò potrebbe non essere quello che si vuole se non si è ancora pronti per l'avanzamento. Se si è già eseguito **apt update**, si può ancora tornare indietro senza problemi seguendo la procedura illustrata in seguito.

Se sono già stati installati pacchetti anche da bullseye, probabilmente non ha più molto senso installare pacchetti da buster. In questo caso si dovrà decidere se si desidera continuare o meno. È possibile il «downgrade» dei pacchetti, ma non è un argomento trattato qui.

Da root, aprire il file sources-list di APT (come ad esempio `/etc/apt/sources.list`) con il proprio editor preferito e si esaminino tutte le righe che cominciano con `deb http:`, `deb https:`, `deb tor+http:`, `deb tor+https:`, `URIs: http:`, `URIs:https`, `URIs: tor+http:` o `URIs: tor+https:`, cercando un riferimento a «`stable`». Se ve n'è qualcuno, si cambi `stable` in `buster`.

Se vi sono righe che cominciano con `deb file:` o `URIs: file:`, si deve controllare da sé se gli indirizzi cui si riferiscono contengono un archivio di buster o di bullseye.

> IMPORTANTE
>
> Non si modifichi alcuna riga che inizia con `deb cdrom:` o `URIs: cdrom:`, in quanto in tal caso si invaliderebbe la riga e si dovrebbe eseguire nuovamente **apt-cdrom**. Non ci si allarmi se una fonte `cdrom:` fa riferimento a «`unstable`»: sebbene sia motivo di confusione, questo è normale.

Se si sono fatte delle modifiche, si salvi il file e si esegua

```
# apt update
```

per aggiornare la lista dei pacchetti.

A.3 Rimuovere file di configurazione obsoleti

Prima di aggiornare il proprio sistema a bullseye, è raccomandata la rimozione dei vecchi file di configurazione (come i file `*.dpkg-{new,old}` in `/etc`) dal sistema.

Appendice B

Contributori delle note di rilascio

Molte persone hanno aiutato per le note di rilascio, inclusi, ma non solo,

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.

Questo documento è stato tradotto in molte lingue. Molte grazie ai traduttori.

Indice analitico