Release-Notes for Debian 13 (trixie)

Debian Documentation Team

2025-08-10

Indice

Il Debian Documentation Project <https://www.debian.org/doc>.

Ultimo aggiornamento il: 2025-08-10

CAPITOLO 1

Introduzione

Questo documento fornisce informazioni agli utenti della distribuzione Debian sui cambiamenti principali nella versione 13 (nome in codice trixie).

Le note di rilascio forniscono informazioni su come aggiornare in modo sicuro dalla versione 12 (nome in codice bookworm) 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/trixie/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 bookworm). 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 bookworm.

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 per il pacchetto **release-notes**. Prima di inviare la segnalazione si dovrebbe verificare se tra le segnalazioni d'errore esistenti 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 *Sorgenti di questo documento* 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 bookworm a trixie è benvenuta. Se si desidera condividere informazioni, compilare una segnalazione nel sistema di tracciamento dei bug 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 *Salvare i dati e le informazioni di configurazione*, 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 *Registrazione della sessione*.
- 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 reStructuredText. La versione HTML viene generata usando *sphinx-build -b html*.. La versione in PDF viene generata usando *sphinx-build -b latex*. I sorgenti delle Note di rilascio sono disponibili nell'archivio Git del *Debian Documentation Project*. È possibile utilizzare l'interfaccia web 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.

CAPITOLO 2

Cosa c'è di nuovo in Debian 13

Il Wiki contiene ulteriori informazioni su questo argomento.

2.1 Architetture supportate

Le seguenti architetture sono ufficialmente supportate da Debian 13:

- PC a 64 bit (`amd64`)
- ARM a 64 bit (`arm64`)
- ARM EABI (`armel`)
- ARMv7 (EABI hard-float ABI, `armhf`)
- PowerPC little-endian a 64 bit (`ppc64el`)
- RISC-V little-endian a 64 bit (`riscv64`)
- IBM System z (`s390x`)

In aggiunta, su sistemi PC a 64 bit, è disponibile uno spazio utente parziale a 32 bit (`i386`). Vedere *Supporto ridotto per i386* per i dettagli.

Vedere *Ultimo rilascio per armel* per le limitazioni del supporto per l'architettura ARM EABI (`armel`).

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.

2.2 Cosa c'è di nuovo nella distribuzione?

2.2.1 Supporto ufficiale per riscv64

Questo rilascio per la prima volta supporta ufficialmente l'architettura riscv64, permettendo agli utenti di eseguire Debian su hardware RISC-V a 64 bit e trarre beneficio da tutte le funzionalità di Debian 13.

Il Wiki fornisce ulteriori dettagli sul supporto di riscv64 in Debian.

2.2.2 Sicurezza rinforzata rispetto ad attacchi ROP e COP/JOP su amd64 e arm64

trixie introduce funzionalità di sicurezza sulle architetture amd64 e arm64 pensate per mitigare exploit Return-Oriented Programming (ROP) e attacchi Call/Jump-Oriented Programming (COP/JOP).

Su amd64 ciò si basa sulla Control-flow Enforcement Technology (CET) di Intel per la protezione da ROP e COP/JOP, su arm64 si basa su Pointer Authentication (PAC) per la protezione da ROP e su Branch Target Identification (BTI) per la protezione da COP/JOP.

Le funzionalità sono abilitate automaticamente se l'hardware le supporta. Per amd64 vedere la documentazione del kernel Linux e la documentazione Intel, e per arm64 vedere il Wiki e la documentazione Arm, che hanno informazioni su come verificare se il proprio processore supporta CET e PAC/BTI e come funzionano.

2.2.3 Supporto per HTTP Boot

L'installatore Debian e le immagini Debian Live possono ora essere avviati usando l'"«HTTP Boot» sul firmware UEFI e U-Boot supportato.

Nei sistemi che usano firmware TianoCore, entrare nel menu *Device Manager*, poi scegliere *Network Device List*, selezionare l'interfaccia di rete, *HTTP Boot Configuration* e specificare l'URL completo della ISO Debian da avviare.

Per altre implementazioni di firmware vedere la documentazione per l'hardware del proprio sistema o la documentazione del firmware.

2.2.4 Traduzioni migliorate per le pagine di manuale

Il progetto *manpages-l10n* ha contribuito molte traduzioni migliorate o nuove per le pagine di manuale. In particolare le traduzioni in rumeno e polacco sono fortemente migliorate rispetto a bookworm.

2.2.5 Supporto per il controllo ortografico in browser web Qt WebEngine

I browser web basati su Qt WebEngine, in particolare Privacy Browser e Falkon, supportano ora il controllo ortografico usando i dati di `hunspell`. I dati sono disponibili nel formato per `dizionari binario BDIC` che è fornito in ogni pacchetto per lingua di Hunspell per la prima volta in Trixie.

Ulteriori informazioni sono disponibili nella segnalazione di bug correlata.

2.2.6 Transizione ABI time_t ABI a 64-bit

Tutte le architetture, eccetto `i386`, usano ora l'ABI `time_t` a 64-bit, per supportare date oltre a 2038.

Nelle architetture a 32 bit (`armel` e `armhf`) l'ABI di molte librerie è cambiata senza cambiare il «soname» della libreria. In queste architetture, il software e i pacchetti di terze parti devono essere ricompilati/rigenerati e deve essere verificata la possibilità di perdite di dati silenti.

L'architettura `i386` non ha preso parte alla transizione, dato che la sua funzione principale è quella di supportare hardware obsoleto.

Ulteriori dettagli possono essere trovati nel wiki Debian.

2.2.7 Progresso di Debian verso compilazioni riproducibili

Coloro che contibuiscono a Debian hanno fatto importanti progressi verso l'assicurazione che le compilazioni dei pacchetti producano risultati riproducibili byte-per-byte. Si può verificare lo stato per i pacchetti installati nel proprio sistema usando il nuovo pacchetto **debian-repro-status**, oppure visitare reproduce.debian.net per le statistiche generale di Debian per trixie e successive.

Si può contribuire a questo processo entrando in `#debian-reproducible` in IRC per discutere risoluzioni di problemi o verificare le statistiche installando il nuovo pacchetto **rebuilderd** e impostando la propria istanza personale.

2.2.8 wcurl e supporto per HTTP/3 in curl

Sia la CLI di CLI sia libcurl supportano ora HTTP/3.

Le richieste HTTP/3 possono essere fatte con le opzioni `--http3` o `--http3-only`.

Il pacchetto **curl** fornisce ora wcurl, un'alternativa a wget che usa curl per effettuare gli scaricamenti.

Scaricare i file è semplice tanto quanto fare `wcurl URL`.

2.2.9 Supporto per dizionari BDIC binari di Hunspell

Trixie fornisce i dizionari binari .bdic compilati da sorgenti Hunspell per la prima volta in Debian. Il formato .bdic è stato sviluppato da Google per l'uso in Chromium. Può essere usato da Qt WebEngine, che è derivato dai sorgenti di Chromium. I browser web basati su Qt WebEngine possono sfruttare i dizionari .bdic forniti, se hanno l'appropriato supporto a monte. Ulteriori informazioni sono disponibili nella correlata segnalazione di bug.

2.2.10 Desktop e pacchetti noti

Questa nuova versione di Debian contiene molto più software rispetto alla precedente, bookworm; la distribuzione include più di 14116 nuovi pacchetti, per un totale di oltre 69830 pacchetti. La maggior parte del software nella distribuzione è stata aggiornata: più di 44326 pacchetti software (corrispondenti al 63% di tutti i pacchetti in bookworm). Inoltre, un notevole numero di pacchetti (oltre 8844, il 12% dei pacchetti in bookworm) 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 *Pacchetti obsoleti*.

Debian viene ancora una volta fornita con molti ambienti e applicazioni desktop. Fra l'altro include ora gli ambienti desktop GNOME 48, KDE Plasma 6.3, LXDE 13, LXQt 2.1.0 e Xfce 4.20.

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

- LibreOffice viene aggiornato alla versione 25;

- GNUcash viene aggiornato a 5.10;

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

Pacchetto	Versione in 12 (bookworm)	Versione in 13 (trixie)
Apache	2.4.62	2.4.64
Bash	5.2.15	5.2.37
Server DNS BIND	9.18	9.20
Cryptsetup	2.6	2.7
curl/libcurl	7.88.1	8.14.1
Emacs	28.2	30.1
Exim (server di posta predefinito)	4.96	4.98
GCC, GNU Compiler Collection (compilatore predefinito)	12.2	14.2
GIMP	2.10.34	3.0.4
GnuPG	2.2.40	2.4.7
Inkscape	1.2.2	1.4
la libreria GNU C	2.36	2.41
Kernel Linux	serie 6.1	6.12 series
Insieme di strumenti LLVM/Clang	13.0.1 e 14.0 (predefinito) e 15.0.6	19 (default), 17 and 18 available
MariaDB	10.11	11.8
Nginx	1.22	1.26
OpenJDK	17	21
OpenLDAP	2.5.13	2.6.10
OpenSSH	9.2p1	10.0p1
OpenSSL	3.0	3.5
Perl	5.36	5.40
PHP	8.2	8.4
Postfix	3.7	3.10
PostgreSQL	15	17
Python 3	3.11	3.13
Rustc	1.63	1.85
Samba	4.17	4.22
Systemd	252	257
Vim	9.0	9.1

2.2.11 Plasma 6

Debian 13 sarà il primo rilascio Debian a fornire Plasma 6. Questo è un importante aggiornamento rispetto a Plasma 5 presente in Debian 12 ed è costruito su uno stack completamente nuovo basato su librerie Qt 6 e KDE Framework 6.

Debian 13 (trixie) fornisce:

- Qt 6.8.2 (aggiornato da 6.4.2)
- KDE Frameworks 6.13 (nuovo)
- Plasma 6.3.6 (sostituisce Plasma 5.27.5)
- Applicazioni KDE Gear:
  - Suite KDE PIM nella versione 24.12.3
  - Altre applicazioni Gear nella versione 25.04.3 (tranne Neochat, KDevelop, Partition Manager)

I dettagli su tutti i pacchetti aggiornati e rimossi nello stack rispetto a Debian 12 in 13 possono essere trovati nella pagina wiki sui Piani di rilascio di Trixie del Team Qt / KDE.

Gli aggiornamenti sul posto dei profili utente sono generalmente supportati, ma sono stati riportati alcuni problemi occasionali. I problemi che non è stato possibile risolvere nella distribuzione vengono tracciati nella pagina wiki sulle stranezza nell'aggiornamento a Plasma 6 insieme alle loro soluzioni.

Per compatibilità con le applicazioni esistenti, Debian 13 fornisce anche:

- Qt 5.15.15 (aggiornato da 5.15.8)
- KDE Frameworks 5.116 (aggiornato da 5.103)

Krita e poche altre applicazioni dipendono ancora da KDE Frameworks 5, ma le KF5 non sono più sviluppate e sono considerate come deprecate dagli autori a monte. Verranno rimosse durante il ciclo di sviluppo di forky.

CAPITOLO 3

Sistema d'installazione

L'installatore Debian è il sistema d'installazione ufficiale per Debian. Offre molti metodi d'installazione. I metodi disponibili per l'installazione in un sistema dipendono dalla sua architettura.

Le immagini dell'installatore per trixie possono essere trovate, insieme alla Guida all'installazione, nel sito web di Debian (https://www.debian.org/releases/trixie/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/language/index.html
```

Si possono anche verificare le errata corrige (all'indirizzo https://www.debian.org/releases/trixie/debian-installer#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 12, raggiungendo un migliore supporto all'hardware e alcune nuove e interessanti funzionalità e migliorie.

Se si è interessati ad una panoramica delle modifiche rispetto a bookworm, controllare gli annunci di rilascio per i rilasci trixie beta e RC disponibili nella cronologia delle notizie dell'Installatore Debian.

3.2 Installare Debian Pure Blend

È ora possibile accedere direttamente dall'installatore ad una selezione di Debian Pure Blend, come Debian Junior, Debian Science o Debian FreedomBox; vedere la installation-guide.

Per informazioni sulle Debian Pure Blends, vedere https://www.debian.org/blends/ o il wiki.

3.3 Installazioni cloud

Il Team cloud pubblica Debian trixie per diversi servizi popolari di cloud computing, inclusi:

- Amazon Web Services
- Microsoft Azure
- OpenStack
- VM semplice

Le immagini cloud forniscono agganci di automazione tramite `cloud-init` e danno priorità ad avvi veloci di istanza usando pacchetti kernel e configurazioni grub specificatamente ottimizzati. Sono fornite, dove appropriato, immagini che supportano diverse architetture e il Team cloud cerca di supportare tutte le funzionalità offerte dal servizio cloud.

Il Team Cloud fornisce immagini aggiornate fino alla fine del periodo LTS di trixie. Vengono tipicamente rilasciate nuove immagini per ogni rilascio minore e dopo risoluzioni di problemi di sicurezza per i pacchetti critici. La politica di supporto completa del Team Cloud è disponibile nella pagina sul Ciclo di vita delle immagini cloud.

Ulteriori dettagli sono disponibili su https://cloud.debian.org/ e nel wiki.

3.4 Immagini per contenitori e macchine virtuali

Immagini contenitore per Debian trixie multi-architettura sono disponibili su Docker Hub. In aggiunta alle immagini standard è disponibile una variante «slim» che riduce l'uso del disco.

CAPITOLO 4

Aggiornamenti da Debian 12 (bookworm)

4.1 Preparazione all'aggiornamento

Prima dell'aggiornamento è consigliato anche leggere le informazioni in *Problemi di cui essere al corrente per trixie*. Tale capitolo copre i potenziali problemi che non sono direttamente correlati al processo di aggiornamento, ma che potrebbe comunque essere 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 di cui si può voler fare il backup sono il contenuto di `/etc`, `/var/lib/dpkg`, `/var/lib/apt/extended_states` e l'output di:

```
$ dpkg --get-selections '*' # (the quotes are important)
```

Se si usa `aptitude` per gestire i pacchetti nel proprio sistema, si vorrà anche fare il backup di `/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 trixie 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 del sistema, come descritto in *Aggiornamento minimo del sistema*, 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 *Aggiornamento del sistema*. 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 la *modalità di ripristino* dell'installatore di Debian trixie. 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 (all'indirizzo https://www.debian.org/releases/trixie/installmanual) e le FAQ dell'installatore di Debian.

[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.

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. 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.

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

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.

Altrimenti 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 /
```

Un altro approccio è quello di abilitare la «shell precoce di debug» di systemd attraverso il `debug-shell.service`. Al successivo avvio il servizio apre una shell di login per root sulla tty9 nei primi momenti del processo di avvio. Può essere abilitata con il parametro di avvio del kernel `systemd.debug-shell=1` oppure essere resa persistente con `systemctl enable debug-shell`, nel qual caso dovrebbe essere nuovamente disabilitata quando il debug è completato.

Ulteriori informazioni su come fare il debug di un avvio non funzionante con systemd possono essere trovate nell'articolo Diagnosing Boot Problems di Freedesktop.org.

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 *Preparazione all'indisponibilità dei servizi*.

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` o `tmux`, 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.

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

Gli utenti del demone watchdog fornito nel pacchetto **micro-evtd** dovrebbero fermare il demone e disabilitare il timer di watchdog prima dell'aggiornamento, per evitare un riavvio spurio nel bel mezzo del processo di aggiornamento:

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

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 bookworm 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.

APT sta passando ad un diverso formato per la configurazione delle fonti da cui scaricare i pacchetti. I file `/etc/apt/sources.list` e `*.list` in `/etc/apt/sources.list.d/` vengono sostituiti da file, sempre in quella directory, ma con nomi che terminano con `.sources`, e che usanoo il nuovo formato (in stile deb822) più comprensibile. Per i dettagli vedere sources.list(5). Gli esempi di configurazioni per APT in questo documento vengono dati nel nuovo formato deb822.

Se il proprio sistema usa più file per le fonti, è necessario assicurarsi che siano coerenti.

4.2.1 Aggiornamento a Debian 12 (bookworm)

Sono supportati solo gli aggiornamenti da Debian 12 (bookworm). Si può visualizzare la propria versione di Debian con:

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

Seguire le istruzioni nelle Note di rilascio per Debian 12 all'indirizzo https://www.debian.org/releases/bookworm/releasenotes per aggiornare prima a Debian 12, se necessario.

4.2.2 Aggiornare all'ultimo rilascio minore

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

4.2.3 Debian Backports

Debian Backports permette agli utenti di Debian stable di eseguire versioni più aggiornate dei pacchetti (con alcuni compromessi rispetto ai test e al supporto di sicurezza). Il Team Debian per Backports mantiene un sottoinsieme di pacchetti dal successivo rilascio di Debian, adattato e ricompilato per l'uso sull'attuale rilascio stabile di Debian.

I pacchetti da bookworm-backports hanno numeri di versione più bassi della versione in trixie, perciò dovrebbero aggiornarsi normalmente a trixie nello stesso modo dei pacchetti bookworm «puri» durante l'aggiornamento della distribuzione. Sebbene non ci siano problemi potenziali noti, i percorsi di aggiornamento da backports sono meno testati e di conseguenza incorrono in più rischi.

Attenzione: Mentre i regolari Debian Backports sono supportati, non c'è un percorso di aggiornamento pulito da backports sloppy (che usano voci per fonti di APT che fanno riferimento a bookworm-backports-sloppy).

Così come per le *Fonti non ufficiali*, si suggerisce agli utenti di rimuovere le voci «bookworm-backports» dai loro file delle fonti per APT prima dell'aggiornamento. Dopo che questo è completato, si può considerare di aggiungere «trixie-backports» (vedere https://backports.debian.org/Instructions/).

Per maggiori informazioni consultare la pagina su Backports del Wiki.

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. Notare che la correzione di questa situazione è possibile solo se i propri file delle fonti per APT puntano tuttora a «bookworm» e non a «stable» o a «trixie». A tale proposito vedere *Controllare la propria configurazione di APT*.

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 Rimozione dei pacchetti non Debian

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

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

4.2.7 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'
```

4.2.8 Le componenti non-free e non-free-firmware

Se si ha firmware non libero installato è raccomandato aggiungere `non-free-firmware` alle proprie fonti di APT.

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

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

4.2.10 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 delle fonti per APT, si dovrebbe controllare che tale archivio offra anche pacchetti compilati per trixie e modificare di conseguenza la voce della fonte contemporaneamente alle voci delle fonti per i pacchetti Debian.

Alcuni utenti potrebbero avere installate nel proprio sistema bookworm 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]. *Possibili problemi durante l'aggiornamento* contiene alcune informazioni su come gestire i conflitti tra file nel caso si verifichino.

4.2.11 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).

4.2.12 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
```

o

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

In alternativa si può anche usare `apt`.

```
# apt list --installed > ~/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.

[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.

```
$ apt-mark showhold
```

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 «hold» (bloccato) di un pacchetto per `apt` può essere modificato eseguendo il comando:

```
# apt-mark hold package_name
```

Sostituire `hold` con `unhold` per disattivare lo stato «hold».

Se c'è bisogno di sistemare qualcosa è meglio controllare che i propri file delle fonti per APT puntino sempre a bookworm come illustrato in *Controllare la propria configurazione di APT*.

4.3 Preparazione dei file delle fonti per APT

Prima di iniziare l'aggiornamento è necessario riconfigurare APT per aggiungere fonti per trixie e tipicamente per rimuovere le fonti per bookworm.

Come detto in *Partire da una Debian «pura»*, è raccomandato l'uso del nuovo formato in stile deb822, perciò si dovrebbero sostituire `/etc/apt/sources.list` e qualsiasi file `*.list` in `/etc/apt/sources.list.d/` con un solo file chiamato `debian.sources` in `/etc/apt/sources.list.d/` (se non è ancora stato fatto). Sotto viene fornito un esempio di come si presenta tipicamente questo file.

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 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 «bookworm», «trixie»), 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 si riceverà una notifica ogni volta che Debian fa un nuovo rilascio, ad esempio come quando «trixie» passa da «testing» a «stable».
- Iscrivendosi alla mailing-list degli annunci di sicurezza di Debian 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 usare il servizio CDN service, la corretta configurazione di APT (presumendo che si stia usando `main` e `non-free-firmware`) è la seguente in `/etc/apt/sources.list.d/debian.sources`:

```
Types: deb
URIs: https://deb.debian.org/debian
Suites: trixie trixie-updates
Components: main non-free-firmware
Signed-By: /usr/share/keyrings/debian-archive-keyring.gpg

Types: deb
URIs: https://security.debian.org/debian-security
Suites: trixie-security
Components: main non-free-firmware
Signed-By: /usr/share/keyrings/debian-archive-keyring.gpg
```

Assicurarsi di aver rimosso ogni vecchio file delle fonti.

Tuttavia, se si hanno risultati migliori usando un mirror specifico che è più vicino in termini di rete invece del servizio CDN, allora l'URI del mirro può essere sostituito nella riga dell'URI con (ad esempio) «URIs: https://mirrors.kernel.org/debian».

Se si desidera usare pacchetti dalle componenti `contrib` o `non-free`, si possono aggiungere questi nomi a tutte le righe `Components:`.

Dopo aver aggiunto le nuove fonti, disabilitare le voci di archivio preesistenti nei file delle fonti di APT, facendole precedere da un simbolo cancelletto (`#`).

4.3.2 Aggiunta di fonti per APT da mirror locale

Anziché usare mirror remoti dei pacchetti, si potrebbe voler modificare i file delle fonti 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/trixie/main/...
/var/local/debian/dists/trixie/contrib/...
```

Per poter utilizzare questo mirror con **apt**, aggiungere la riga seguente al proprio file `/etc/apt/sources.list.d/debian.sources`:

```
Types: deb
URIs: file:/var/local/debian
Suites: trixie
Components: main non-free-firmware
Signed-By: /usr/share/keyrings/debian-archive-keyring.gpg
```

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

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 delle fonti 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    # this will mount the CD to the mount point
# ls -alF /media/cdrom  # this should show the CD's root directory
# umount /media/cdrom   # this will unmount the 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 /mountpoint
```

In seguito si dovrebbe riverificare che le voci delle fonti per APT (nei file in `/etc/apt/sources.list.d/`) facciano riferimento a «trixie» o a «stable». Non dovrebbe esserci alcuna voce per le fonti che punti a bookworm.

Nota: Qualche volta le righe delle fonti per un CD-ROM potrebbero fare riferimento a «`unstable`»; sebbene ciò possa generare confusione *non* devono essere modificate.

4.4.1 Registrazione della sessione

`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 verifica un problema si disporrà di una registrazione di quanto accaduto e, se necessario, si potranno fornire le informazioni esatte in una'eventuale segnalazione di errori.

`term.log` permette anche di rileggere le informazioni scorse fuori dalla schermata. Se si usa la console di sistema, basta passare a VT2 (con `Alt+F2`) per leggerle.

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
```

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 *Aggiornamento del sistema*. Per prima cosa, poiché ogni pacchetto necessario per l'installazione prelevato dalla rete è archiviato in `/var/cache/apt/archives` (e nella sottodirectory `partial/`, durante lo scaricamento), perciò 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, ci si potrebbe ritrovare 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 upgraded, XXX newly installed, XXX to remove and XXX not upgraded.
Need to get xx.xMB of archives.
After this operation, AAAMB of additional disk space will be used.
```

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 *Aggiornamento minimo del sistema* 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: You don't have enough free space in /var/cache/apt/archives/.
```

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 bookworm, 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 usare `debfoster` per trovare pacchetti superflui. Non rimuovere alla cieca i pacchetti indicati da questo strumento, specialmente se si stanno usando opzioni non predefinite aggressive che è possibile diano falsi positivi. È altamente raccomandato fare una revisione manuale dei pacchetti suggeriti per la rimozione (cioè del loro contenuto, dimensione e descrizione) prima di rimuoverli effettivamente.

- 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 *Aggiornamento minimo del sistema*) 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.

Notare che per rimuovere pacchetti in modo sicuro è preferibile tornare a far puntare i propri file delle fonti di APT a bookworm, come descritto in *Controllare la propria configurazione di APT*.

4.4.4 Fermare i sistemi di monitoraggio

Dato che `apt` può avere necessità di fermare temporaneamente servizi in esecuzione sul computer, è probabilmente una buona idea fermare i servizi di monitoraggio che possono riavviare altri servizi terminati durante l'aggiornamento. In Debian, un esempio di tale servizio è **monit**.

4.4.5 Aggiornamento minimo del sistema

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 *Aggiornamento del sistema*.

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.

4.4.6 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 trixie.

4.5.1 Full-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: Could not perform immediate configuration on 'package'.  Please see man 5 apt.conf␣
↪under APT::Immediate-Configure for details.
```

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 temporaneamente entrambe le fonti bookworm e trixie ai propri file delle fonti di APT ed eseguire `apt update`.

4.5.2 Rimozioni attese

Il processo d'aggiornamento a trixie 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 trixie vedere *Pacchetti obsoleti*.

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 package_name
```

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 /path/to/package_name.deb
```

4.5.4 Conflitti tra file

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

```
Unpacking <package-foo> (from <package-foo-file>) ...
dpkg: error processing <package-foo> (--install):
trying to overwrite `<some-file-name>',
which is also in package <package-bar>
dpkg-deb: subprocess paste killed by signal (Broken pipe)
Errors were encountered while processing:
<package-foo>
```

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 package_name
```

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 bookworm a trixie 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 *Cose da fare prima di riavviare* 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, 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 *Aggiornamento minimo del sistema*.

4.6.2 Dimensione di pagina per PowerPC (ppc64el) little-endian a 64-bit

A partire da trixie, il kernel Linux predefinito per l'architettura ppc64el (pacchetto **linux-image-powerpc64le**) usa una dimensione delle pagine di memoria di 4kiB invece dei precedenti 64 kiB. Ciò corrisponde ai valori per le altre architetture comuni e evita alcune incompatibilità con dimensioni di pagina più grandi nel kernel (in particolare i driver `nouveau` e `xe`) e con applicazioni in spazio utente. In generale ci si aspetta che ciò riduca l'uso di memoria e aumenti leggermente l'uso della CPU.

Viene fornito un pacchetto del kernel alternativo (**linux-image-powerpc64le-64k**) che usa una dimensione di pagina di 64kiB. Sarà necessario installare questo pacchetto alternativo se:

- È necessario eseguire macchine virtuali con una dimensione di pagina di 64kiB.

  Vedere anche *Problemi con VM su PowerPC little-endian a 64-bit (ppc64el)*.

- È necessario usare la compressione PowerPC Nest (NX).
- Si usa un file system con una dimensione dei blocchi > 4kiB (4096 bytes). Ciò è probabile se si sta usando Btrfs. Lo si può verificare con:
  - Btrfs: `file -s device | grep -o 'sectorsize [0-9]*'`
  - ext4: `tune2fs -l device | grep '^Block size:'`
  - XFS: `xfs_info device | grep -o 'bsize=[0-9]*`

Per alcune applicazioni, come server di database, usare una dimensione di pagina di 64kiB può fornire prestazioni migliori e questo pacchetto del kernel alternativo può essere preferibile rispetto a quello predefinito.

4.7 Pulizia dopo l'aggiornamento

Sono raccomandate due azioni per pulire la distribuzione aggiornata.

- Si rimuovano i pacchetti ora obsoleti o ridondanti come descritto in *Accertarsi di avere spazio disponibile a sufficienza per l'aggiornamento* e *Pacchetti obsoleti*. 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 *Eliminare completamente i pacchetti rimossi*.
- Aggiornare le proprie fonti di APT. APT sta rendendo deprecato il vecchio formato usato per specificare quali repository usare. Vedere *Preparare i file delle fonti di APT* e sources.list(5). Se non sono stati ancora cambiati tutti i propri file di configurazione, si può usare la nuova funzionalità `apt modernize-sources` di `apt`.

4.8 Ripulire i pacchetti installati automaticamente.

Alcuni pacchetti possono essere stati installati nel sistema solamente come dipendenze di altri pacchetti. Con il nuovo rilascio, queste dipendenze possono essere cambiate e apt proporrà la rimozione di questi pacchetti installati automaticamente. Per farlo eseguire:

```
# apt autoremove
```

4.9 Pacchetti obsoleti

trixie introduce moltissimi nuovi pacchetti, ma nel contempo ritira e manca di alcuni vecchi pacchetti che erano presenti in bookworm. 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 trixie[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 trixie a causa di errori. In quest'ultimo caso, i pacchetti potrebbero continuare a essere presenti nella distribuzione «unstable».

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

I «Pacchetti obsoleti o creati localmente» possono essere elencati ed eliminati completamente usando la riga di comando con:

```
$ apt list '~o'
# apt purge '~o'
```

Il Sistema di tracciamento dei bug (BTS) di Debian 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.

Per un elenco dei pacchetto obsoleti per trixie fare riferimento a *Pacchetti obsoleti degni di nota*.

4.9.1 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 bookworm) 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:

```
$ apt list '~c'
```

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 '~c'
```

4.9.2 Pacchetti fittizi di transizione

Alcuni pacchetti da bookworm possono essere stati sostituiti in trixie 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.

CAPITOLO 5

Problemi di cui essere al corrente per trixie

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 *Ulteriori letture*.

5.1 Cose da sapere quando si aggiorna a trixie

Questa sezione tratta le voci relative all'aggiornamento da bookworm a trixie.

5.1.1 Aggiornamenti remoti interrotti

Un problema in OpenSSH in bookworm può portare a sistemi remoti non accessibili, se un aggiornamento pilotato attraverso una connessione SSH viene interrotto. Gli utenti potrebbero non essere in grado di riconnettersi al sistema remoto per riprendere l'aggiornamento.

I pacchetti aggiornati per bookworm risolvono questo problema in Debian 12.12, ma questo rilascio era ancora in fase di preparazione al momento del rilascio di trixie. Agli utenti che hanno in programma di aggiornare sistemi remoti attraverso una connessione SSH, viene suggerito invece di aggiornare prima OpenSSH alla versione 1:9.2p1-2+deb12u7 o ad una successiva, attraverso il meccanismo stable-updates .

5.1.2 Supporto ridotto per i386

A partire da trixie, i386 non è più supportata come architettura regolare; non c'è alcun kernel ufficiale o installatore Debian per i sistemi i386. Meno pacchetti sono disponibili per i386 perché molti progetti non la supportano più. L'unico scopo restante dell'architettura è quello di supportare l'esecuzione di codice obsoleto, per esempio utilizzando il multiarch o una chroot in un sistema a 64 bit (amd64).

L'architettura i386 è ora pensata solamente per l'uso su una CPU a 64 bit (amd64). I requisiti del suo insieme di istruzioni includono il supporto per SSE2, perciò non potrà essere eseguita con successo sulla maggior parte dei tipi di CPU a 32 bit che erano supportati da Debian 12.

Gli utenti che eseguono sistemi i386 non dovrebbero aggiornare a trixie. Debian raccomanda invece di reinstallarli come amd64, dove possibile, o di mettere in disuso l'hardware. Il Cross-grading senza una reinstallazione è un'alternativa tecnicamente possibile, ma rischiosa.

5.1.3 Ultimo rilascio per armel

A partire da trixie, armel non è più supportata come architettura regolare: non c'è alcun installatore Debian per i sistemi armel e solo Raspberry Pi 1, Zero e Zero W sono supportate dai pacchetti del kernel.

Gli utenti che eseguono sistemi armel possono aggiornare a trixie, purché il loro hardware sia supportato nei pacchetti del kernel oppure se usano un kernel di terze parti.

trixie sarà l'ultimo rilascio per l'architettura armel. Debian raccomanda, quando possibile, di reinstallare i sistemi armel come armhf o arm64, oppure di mettere l'hardware in disuso.

5.1.4 Architetture MIPS rimosse

A partire da trixie, le architetture *mipsel* e *mips64el* non sono più supprtate da Debian. Agli utenti di queste architetture viene suggerito di passare ad un'architettura diversa.

5.1.5 Assicurarsi che /boot abbia abbastanza spazio libero

I pacchetti del kernel Linux e del firmware sono aumentati notevolmente di dimensione nei precedenti rilasci di Debian e in trixie. Come conseguenza la partizione `/boot` potrebbe essere troppo piccola causando il fallimento dell'aggiornamento. Se il sistema è stato installato con Debian 10 (buster) o precedenti, è molto probabile che il sistema risenta di questo problema.

Prima di avviare l'aggiornamento, assicurarsi che la propria partizone `/boot` abbia una dimensione di almeno 768 MB e che abbia circa 300 MB liberi. Se il proprio sistema non ha una partizione `/boot` separata, non dovrebbe essere necessario fare nulla.

Se `/boot` è in LVM ed è troppo piccola, si può usare `lvextend` per aumentare la dimensione di una partizione LVM. Se `/boot` è una partizione separata è probabilmente più facile reinstallare il sistema.

5.1.6 La directory dei file temporanei /tmp è ora memorizzata in un tmpfs

A partire da trixie, la directory `/tmp/` è archiviata in modo predefinito in memoria usando un file system tmpfs(5). Ciò dovrebbe rendere più veloci le applicazioni che usano file temporanei, ma se ci vengono messi file grandi si può esaurire la memoria.

Per i sistemi aggiornati da bookworm, il nuovo comportamento inizia solo dopo un riavvio. I file lasciati in `/tmp` vengono nascosti dopo che il nuovo *tmpfs* è montato, il che genera avvertimenti nel giornale di sistema o in syslog. Si può accedere a tali file usando bind-mount (vedere mount(1)): eseguire `mount --bind / /mnt` rende possibile accedere alla directory sottostante in `/mnt/tmp` (eseguire `umount /mnt` dopo che sono stati ripuliti i file vecchi).

Il comportamento predefinito è allocare fino al 50% della memoria a `/tmp` (questo è un valore massimo: la memoria viene usato solamente quando vengono effettivamente creati i file in `/tmp`). Questa dimensione può essere modificata eseguendo `systemctl edit tmp.mount` come root e impostando, ad esempio:

```
[Mount]
Options=mode=1777,nosuid,nodev,size=2G
```

(vedere systemd.mount(5)).

Si può tornare ad avere `/tmp` come directory regolare eseguendo `systemctl mask tmp.mount` come root e riavviando.

Le nuove impostazioni predefinite per il file system possono essere scavalcate in `/etc/fstab`, perciò i sistemi che hanno già definito una partizione `/tmp` separata non verranno toccati.

5.1.7 openssh-server non legge più ~/.pam_environment

Il demone Secure Shell (SSH) fornito nel pacchetto **openssh-server**, che permette il login da sistemi remoti, non legge più in modo predefinito il file `~/.pam_environment` degli utenti; questa funzionalità ha problemi storici di sicurezza ed è stata deprecata nelle attuali versioni della libreria Pluggable Authentication Modules (PAM) library. Se si usava questa funzionalità, si dovrebbe passare dall'impostare le variabili in `~/.pam_environment` all'impostarle invece nei propri file di inizializzazione della shell (es. `~/.bash_profile` o `~/.bashrc`) o qualche altro meccanismo simile.

La cosa non ha effetto sulle connessioni SSH esistenti, ma le nuove connessioni possono comportarsi in modo diverso dopo l'aggiornamento. Se si sta facendo l'aggiornamento da remoto, è normalmente una buona idea assicurarsi di avere un qualche altro modo per fare il login nel sistema prima di avviare l'aggiornamento; vedere *Preparazione per il ripristino*.

5.1.8 OpenSSH non supporta più le chiavi DSA

Le chiavi Digital Signature Algorithm (DSA), come specificate nel protocollo Secure Shell (SSH), sono intrinsecamente deboli: sono limitate a chiavi private a 160 bit e a SHA-1 digest. L'implementazione di SSH fornita dai pacchetti **openssh-client** e **openssh-server** ha il supporto per le chiavi DSA disabilitato a partire da OpenSSH 7.0p1 nel 2015, rilasciato con Debian 9 («stretch»), sebbene potesse ancora essere abilitato usando le opzioni di configurazione `HostKeyAlgorithms` e `PubkeyAcceptedAlgorithms`, rispettivamente per le chiavi dell'host e dell'utente.

A questo punto l'unico uso restante di DSA dovrebbe essere quello di connettersi a un qualche dispositivo molto vecchio. Per tutti gli altri usi, gli altri tipi di chiave supportati da OpenSSH (RSA, ECDSA e Ed25519) sono migliori.

A partire da OpenSSH 9.8p1 in trixie, le chiavi DSA non sono più supportate neanche con le opzioni di configurazione descritte sopra. Se si ha un dispositivo a cui ci si può connettere solo usando DSA, allora per farlo si può usare il comando `ssh1` fornito dal pacchetto **openssh-client-ssh1**.

Nella remota eventualità che si stia ancora usando chiavi DSA per connettersi ad un server Debian (se non si è sicuri si può controllare aggiungendo l'opzione `-v` alla riga di comando di `ssh` utilizzata per connettersi a quel server e cercare

la riga «Server accepts key:»), si devono generare chiavi sostitutive prima di fare l'aggiornamento. Per esempio, per generare una nuova chiave Ed25519 e abilitare il login ad un server usando quella, eseguire quanto segue nel client, sostituendo ad `username@server` i nomi appropriati per utente e host:

```
$ ssh-keygen -t ed25519
$ ssh-copy-id username@server
```

5.1.9 I comandi last, lastb e lastlog sono stati rimpiazzati

Il pacchetto **util-linux** non fornisce più i comandi `last` e `lastb`, e il pacchetto **login** non fornisce più `lastlog`. Questi comandi fornivano informazioni sui tentativi di login precedenti usando `/var/log/wtmp`, `/var/log/btmp`, `/var/run/utmp` e `/var/log/lastlog`, ma questi file non saranno usabili dopo il 2038 perché non allocano spazio sufficiente per l'orario di connessione (il Year 2038 Problem), e gli sviluppatori a monte non vogliono cambiare i formati dei file. La maggior parte degli utenti non avrà necessità di cambiare questi comandi con null'altro, ma il pacchetto **util-linux** fornisce un comando `lslogins` che può dire quali account sono stati usati più recentemente.

Sono disponibili due sostituti diretti: `last` può essere rimpiazzato da `wtmpdb` dal pacchetto **wtmpdb** (deve essere installato anche il pacchetto **libpam-wtmpdb**) e `lastlog` può essere rimpiazzato da `lastlog2` dal pacchetto **lastlog2** (deve essere installato anche **libpam-lastlog2**). Se si desidera usare uno di questi, è necessario installare i nuovi pacchetti dopo l'aggiornamento, vedere NEWS.Debian di util-linux per ulteriori informazioni. Il comando `lslogins --failed` fornisce informazioni simili a `lastb`.

Se si installa **wtmpdb**, allora è raccomandato rimuovere i vecchi file di log `/var/log/wtmp*`. Se si installa **wtmpdb**, questo aggiorna `/var/log/wtmp` e si possono leggere i vecchi file wtmp con `wtmpdb import -f <dest>`. Non esiste uno strumento per leggere il file `/var/log/lastlog*` o `/var/log/btmp*`: questi possono essere rimossi dopo l'aggiornamento.

5.1.10 I file system cifrati necessitano del pacchetto systemd-cryptsetup

Il supporto per il rilevamento e il montaggio automatico dei file system cifrati è stato spostato nel nuovo pacchetto **systemd-cryptsetup**. Questo nuovo pacchetto è raccomandato da **systemd**, perciò dovrebbe essere installato automaticamente con l'aggiornamento.

Se si usano file system cifrati, assicurarsi che il pacchetto **systemd-cryptsetup** sia installato prima di riavviare.

5.1.11 Le impstazioni predefinite di cifratura per dispositivi dm-crypt in plain-mode sono cambiate

Le impostazioni predefinite per i dispositivi `dm-crypt` creati usando la cifratura in modalità `plain` (vedere crypttab(5)) sono cambiate per migliorare la sicurezza. Ciò crea problemi le impostazioni usate non sono state memorizzate in `/etc/crypttab`. Il modo raccomandato per configurare i dispositivi in plain-mode è di registrare le opzioni `cipher`, `size` e `hash` in `/etc/crypttab`. in caso contrario `cryptsetup` usa i valori predefiniti e quelli predefiniti per gli algoritmi di cifratura e di hash sono cambiati in trixie, e questo farà sì che tali dispositivi appaiano come dati casuali fino a che non sono configurati correttamente.

Ciò non vale per i dispositivi LUKS, perchè LUKS memorizza le impostazioni nel dispositivo stesso.

Per configurare correttamente i propri dispositivi plain-mode, presumendo che siano stati creati con i valori predefiniti di bookworm, aggiungere `cipher=aes-cbc-essiv:sha256,size=256,hash=ripemd160` a `/etc/crypttab`.

Per accedere a tali dispositivi con `cryptsetup` dalla riga di comando, si può usare `--cipher aes-cbc-essiv:sha256 --key-size 256 --hash ripemd160`. Debian raccomanda di configurare i dispositivi permanenti con LUKS, oppure se si usa la modalità plain mode, di memorizzare in modo esplicito tutte le

opzioni di cifratura necessarie in `/etc/crypttab`. I nuovi valori predefiniti sono `cipher=aes-xts-plain64` e `hash=sha256`.

5.1.12 RabbitMQ non supporta più le code HA

A partire da trixie le code High-availability (HA) non sono più supportate da **rabbitmq-server**. Per continuare ad usare una configurazione HA, queste code devono essere convertite in «code quorum».

Se si ha una installazione OpenStack, cambiare le code a quorum prima dell'aggiornamento. Notare anche che a partire dal rilascio «Caracal» di OpenStack in trixie, OpenStack supporta solo code quorum.

5.1.13 RabbitMQ non può essere aggiornato direttamente da bookworm

Non esiste un percorso di aggiornamento facile e diretto per RabbitMQ da bookworm a trixie. I dettagli relativi a questo problema possono essere trovati nel bug 1100165.

Il percorso di aggiornamento raccomandato è quello di eliminare completamente il database di rabbitmq database e riavviare il servizio (dopo l'aggiornamento a trixie). Ciò può essere fatto eliminando `/var/lib/rabbitmq/mnesia` e tutto il suo contenuto.

5.1.14 Gli aggiornamenti della versione principale di MariaDB funzionano in modo affidabile solo dopo uno spegnimento pulito.

MariaDB non supporta il ripristino da errori attraverso versioni maggiori diverse. Per esempio, se un server MariaDB 10.11 ha subito uno spegnimento improvviso a causa di una interruzione di alimentazione o di un problema software, il database deve essere riavviato con gli stessi binari MariaDB 10.11 in modo che possa fare il ripristino dagli errori con successo e possa riconciliare i file dei dati e i file di log per portare avanti o annullare le transazioni che sono state interrotte.

Se si cerca di fare il ripristino da un crash con MariaDB 11.8 usando la directory dei dati da un'istanza di MariaDB 10.11 andata in cash, il nuovo server MariaDB si rifiuterà di avviarsi.

Per assicurarsi che un server MariaDB venga spento in maniera pulita prima di fare un aggiornamento della versione principale, fermare il servizio con

```
# service mariadb stop
```

e in seguito controllare i log del server cercando `Shutdown complete` per confermare che tutti i dati e i buffer siano stati svuotati su disco con pieno successo.

Se non è stato spento in modo pulito, riavviarlo per attivare il recupero dai crash, poi fermarlo di nuovo e controllare che il secondo spegnimento sia stato pulito.

Per informazioni aggiunti su come fare backup e altre informazioni correlate per gli amministratori di sistema, vedere /usr/share/doc/mariadb-server/README.Debian.gz.

5.1.15 Ping non viene più eseguito con privilegi elevati

La versione predefinita di ping (fornita da **iputils-ping**) non è più installata con accesso alla capacità Linux *CAP_NET_RAW*, ma usa invece socket datagram `ICMP_PROTO` per la comunicazione di rete. L'accesso a questi socket è controllato sulla base dell'appartenenza a gruppi Unix dell'utente usando il sysctl `net.ipv4.ping_group_range`. In installazioni normali, il pacchetto **linux-sysctl-defaults** imposta questo valore ad un valore molto permissivo, permettendo agli utenti non privilegiati di usare ping come atteso, ma alcuni scenari di aggiornamento possono non installare automaticamente questo pacchetto. Vedere `/usr/lib/sysctl.d/50-default.conf` e la documentazione del kernel per maggiori informazioni sulle specifiche di questa variabile.

5.1.16 I nomi delle interfacce di rete possono cambiare

Agli utenti di sistemi senza una facile gestione fuori banda (out-of-band) viene suggerito di procedere con cautela, dato che sono note due circostanze in cui i nomi delle interfacce di rete assegnate dai sistemi trixie possono essere diversi da bookworm. Ciò può far sì che la connettività di rete non funzioni quando si riavvia per completare l'aggiornamento.

È difficile determinare in anticipo se un dato sistema sarà affetto da questo problema, senza un'analisi tecnica dettagliata. Le configurazioni che sono note per essere problematiche sono:

- Sistemi che usano il driver NIC Linux **i40e**, vedere bug n. 1107187.
- Sistemi in cui il firmware espone l'oggetto tabella ACPI `_SUN` che veniva precedentemente ignorato in modo predefinito in bookworm (systemd.net-naming-scheme v252), ma che p ora usato da **systemd** v257 in trixie. Vedere bug n.1092176.

  Si può usare il comando `$ udevadm test-builtin net_setup_link` per vedere se il solo cambio di systemd produrrebbe un nome diverso. Ciò deve essere fatto immediatamente prima di riavviare per finire l'aggiornamento. Per esempio:

```
# After apt full-upgrade, but before reboot
$ udevadm test-builtin net_setup_link /sys/class/net/enp1s0 2>/dev/null
ID_NET_DRIVER=igb
ID_NET_LINK_FILE=/usr/lib/systemd/network/99-default.link
ID_NET_NAME=ens1  #< Notice the final ID_NET_NAME name is not "enp1s0"!
```

Agli utenti che hanno bisogno che i nomi rimangano fissi durante l'aggiornamento viene suggerito di creare file systemd.link per «fermare (pin)» il nome attuale prima dell'aggiornamento.

5.1.17 Modifiche alla configurazione di Dovecot

La suite per server di posta **dovecot** in trixie usa un formato di configurazione che è incompatibile con le versioni precedenti. Dettagli sulle modifiche alla configurazione sono disponibili su docs.dovecot.org.

Allo scopo di evitare un tempo di indisponibilità esteso, è caldamente incoraggiato fare la transizione della propria configurazione in un ambiente di prova prima di iniziare l'aggiornamento di un sistema di posta usato in produzione.

Notare anche che alcune funzionalità sono state rimosse nel codice a monte in v2.4. In particolare, *replicator* non c'è più. Se si dipende da quella funzione, è consigliabile non aggiornare a trixie fino a che non è stata trovata un'alternativa.

5.1.18 Modifiche importanti alla pacchettizzazione di libvirt

Il pacchetto **libvirt-daemon**, che fornisce un'API e un toolkit per gestire piattaforme di virtualizzazione, è stato ristrutturato in trixie. Ogni backend per archiviazione e driver viene ora fornito in un pacchetto binario distinto, il che fornisce una flessibilità molto maggiore.

Viene fatta attenzione durante gli aggiornamenti a bookworm a mantenere l'insieme esistente dei componenti, ma in alcuni casi può essere temporaneamente persa qualche funzionalità. È raccomandato rivedere con attenzione l'elenco dei pacchetti binari installati dopo l'aggiornamento, per assicurarsi che siano presenti tutti quelli attesi; questo è anche un ottimo momento per considerare la disinstallazione dei componenti non desiderati.

In aggiunta alcuni file di configurazione possono diventare contrassegnati come «obsoleti» dopo l'aggiornamento. Il file `/usr/share/doc/libvirt-common/NEWS.Debian.gz` contiene informazioni aggiuntive su come verificare se il proprio sistema è affetto da questo problema e su come risolverlo.

5.1.19 Samba: modifiche nella pacchettizzazione di Active Directory Domain Controller

La funzionalità Active Directory Domain Controller (AD-DC) è stata scorporata da **samba**. Se si usa tale funzionalità è necessario installare il pacchetto **samba-ad-dc**.

5.1.20 Samba: moduli VFS

Il pacchetto **samba-vfs-modules** è stato riorganizzato. La maggior parte dei moduli VFS è ora inclusa nel pacchetto **samba**. Tuttavia i moduli per *ceph* e *glusterfs* sono stati separati in **samba-vfs-ceph** e **samba-vfs-glusterfs**.

5.1.21 OpenLDAP TLS è ora fornito da OpenSSL

Il supporto per TLS nel client OpenLDAP **libldap2** e nel server **slapd** è ora fornito da OpenSSL, invece che da GnuTLS. Ciò influenza sia le opzioni di configurazioni disponibili, sia il loro comportamento.

I dettagli sulle opzioni cambiate possono essere trovati in `/usr/share/doc/libldap2/NEWS.Debian.gz`.

Se non è specificato alcun certificato TLS CA, l'archivio di fiducia («trust store») predefinito di sistema viene ora caricato automaticamente. Se non si desidera che vengano usate le CA predefinite, è necessario configurare esplicitamente le CA fidate.

Per maggiori informazioni sulla configurazione del client LDAP, vedere la pagina di manuale ldap.conf.5. Per il server LDAP (**slapd**), vedere `/usr/share/doc/slapd/README.Debian.gz` e la pagina di manuale slapd-config.5.

5.1.22 bacula-director: l'aggiornamento dello schema del database richiede grandi quantità di spazio su disco e di tempo

Il database di Bacula subirà una sostanziale modifica dello schema durante l'aggiornamento a trixie.

L'aggiornamento del database può richiedere molte ore, o persino giorni, a seconda della dimensione del database e delle prestazioni del server di database in uso.

L'aggiornamento richiede temporaneamente circa il doppio dello spazio su disco attualmente usato nel server di database, più spazio sufficiente a contenere un dump di backup del database di Bacula in `/var/cache/dbconfig-common/backups`.

Se si finisce lo spazio disponibile durante l'aggiornamento, il database può risultare corrotto e ciò impedisce all'installazione di Bacula di funzionare correttamente.

5.1.23 dpkg: warning: unable to delete old directory: ...

Durante l'aggiornamento, `dpkg` emette avvertimenti simili a questi, per vari pacchetti. Ciò è dovuto alla finalizzazione del progetto `usrmerge`, e tali avvertimenti possono essere ignorati senza problemi.

```
Unpacking firmware-misc-nonfree (20230625-1) over (20230515-3) ...
dpkg: warning: unable to delete old directory '/lib/firmware/wfx': Directory not empty
dpkg: warning: unable to delete old directory '/lib/firmware/ueagle-atm': Directory not␣
↪empty
```

5.1.24 Gli aggiornamenti con salto non sono supportati

Come per ogni altro rilascio Debian, gli aggiornamenti devono essere fatti dal rilascio precedente. Inoltre dovrebbe essere stato installato ogni aggiornamento minore. Vedere *Partire da una Debian «pura»*.

Saltare rilasci durante l'aggiornamento è esplicitamente non supportato.

Per trixie, la finalizzazione del progetto `usrmerge` richiede che l'aggiornamento a bookworm sia completato prima di iniziare l'aggiornamento a trixie.

5.1.25 WirePlumber ha un nuovo sistema di configurazione

WirePlumber ha un nuovo sistema di configurazione. Per la configurazione predefinita, non è necessario fare nulla; per le configurazioni personalizzate vedere `/usr/share/doc/wireplumber/NEWS.Debian.gz`.

5.1.26 Migrazione di strongSwan ad un nuovo demone charon

La suite IKE/IPsec strongSwan migra dal vecchio comando **charon-daemon** (con uso del comando ipsec(8) e configurato in `/etc/ipsec.conf`) a **charon-systemd** (gestitoi con gli strumenti swanctl(8) e configurato in `/etc/swanctl/conf.d`). La versione trixie del metapacchetto **strongswan** richiama le nuove dipendenze, ma le installazioni esistenti non vengono toccate fino a che viene mantenuto installato **charon-daemon**. Si consiglia agli utenti di migrare la propria installazione alla nuova configurazione seguendo quanto descritto nella pagina originale a monte sulla migrazione.

5.1.27 Proprietà di udev da sg3-utils mancanti

A causa del bug n. 1109923 in **sg3-utils** i dispositivi SCSI non ricevono tutte le proprietà nel database «udev». Se la propria installazione fa affidamento sull'iniezione di proprietà da parte del pacchetto* **sg3-utils-udev**, migrare a non usarle oppure prepararsi a fare il debug degli errori di operazioni fallite dopo il riavvio in trixie.

5.1.28 Cose da fare prima di riavviare

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

5.2 Cosa non limitate al processo di aggiornamento

5.2.1 Le directory /tmp e /var/tmp vengono ora pulite regolarmente

Nelle installazioni nuove, *systemd-tmpfiles* elimina regolarmente i vecchi file in `/tmp` e `/var/tmp` quando il sistema è in esecuzione. Questa modifica rende Debian coerente con altre distribuzioni. Dato che esiste un piccolo rischio di perdita di dati, è stato messo come meccanismo «opt-in» (scelto attivamente): l'aggiornamento a trixie crea un file /etc/tmpfiles.d/tmp.conf che reimposta il vecchio comportamento. Questo file può essere cancellato per adottare il nuovo comportamento predefinito, oppure modificato per definire regole personalizzate. Il resto di questa sezione spiega il nuovo comportamento predefinito e come personalizzarlo.

Il nuovo comportamento predefinito prevede la cancellazione automatica dei file in `/tmp` dopo 10 giorni dal momento in cui sono stati usati l'ultima volta (così come dopo un riavvio). I file `/var/tmp` sono cancellati dopo 30 giorni (ma non dopo un riavvio).

Prima di adottare il nuovo comportamento predefinito, si dovrebbe adattare ogni programma locale che memorizza dati in `/tmp` o `/var/tmp` per lunghi periodi di tempo in modo che usi posizioni alternative quali `~/tmp/`, oppure dire a *systemd-tmpfiles* di escludere dalla cancellazione i file creando un file `local-tmp-files.conf` in `/etc/tmpfiles.d` contenente righe simili a:

```
x /var/tmp/my-precious-file.pdf
x /tmp/foo
```

Vedere systemd-tmpfiles(8) e tmpfiles.d(5) per maggiori informazioni.

5.2.2 Messaggio di systemd: System is tainted: unmerged-bin

La versione a monte di systemd, a partire dalla versione 256, considera i sistemi che hanno directory `/usr/bin` e `/usr/sbin` separate come degni di attenzione. All'avio systemd produce un messaggio per registrare questo fatto: `System is tainted: unmerged-bin`.

Viene raccomandato di ignorare questo messaggio. L'unione manuale di queste directory non è supportata e renderà non funzionanti gli aggiornamenti futuri. Ulteriori dettagli possono essere trovati nel bug n. 1085370.

5.2.3 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.

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

Debian 13 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. Le applicazioni che usano il pacchetto sorgente **webkit2gtk** (es. **epiphany**) sono coperte dal supporto di sicurezza, ma le applicazioni che usano qtwebkit (pacchetto sorgente **qtwebkit-opensource-src**) non lo sono.

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.

Una volta che un rilascio diventa `oldstable`, i browser ufficialmente supportati possono non continuare a ricevere aggiornamenti per il periodo di copertura ufficiale. Per esempio, Chromium riceverà solo 6 mesi di supporto di sicurezza in `oldstable` invece dei tipici 12 mesi.

Pacchetti basati su Go e Rust

L'infrastruttura Debian attualmente ha problemi con la ricompilazione di pacchetti del tipo che usa sistematicamente link statici. Con la crescita degli ecosistemi Go e Rust ciò significa che questi pacchetti saranno coperti da un supporto di sicurezza limitato, fino a che l'infrastruttura non sarà migliorata per poter lavorare con essi in modo mantenibile.

Nella maggior parte dei casi, se sono necessari aggiornamenti alle librerie di sviluppo di Go e Rust, questi verranno rilasciati solamente attraverso i regolari rilasci minori.

5.2.4 Problemi con VM su PowerPC little-endian a 64-bit (ppc64el)

Attualmente QEMU cerca sempre di configurare le macchine virtuali PowerPC in modo da supportare pagine di memoria di 64kiB. Questo non funziona con macchine virtuali con accelerazione KVM quando si usa il pacchetto del kernel predefinito.

- Se il sistema operativo ospite usa una dimensione di pagina di 4kiB, si dovrebbe impostare la proprietà della macchina `cap-hpt-max-page-size=4096`. Per esempio:

```
$ kvm -machine pseries,cap-hpt-max-page-size=4096 -m 4G -hda guest.img
```

- Se il sistema operativo ospite richiede una dimensione di pagina di 64kiB, si dovrebbe installare il pacchetto **linux-image-powerpc64le-64k**; vedere *Dimensione di pagina per PowerPC (ppc64el) little-endian a 64-bit*.

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 *Pacchetti obsoleti* per una descrizione).

L'elenco dei pacchetti obsoleti comprende:

- Il pacchetto **libnss-gw-name** è stato rimosso da trixie. Lo sviluppatore originale a monte suggerisce di usare invece **libnss-myhostname**.
- Il pacchetto **pcregrep** è stato rimosso da trixie. Può essere sostituito con `grep -P` (`--perl-regexp`) o `pcre2grep` (da **pcre2-utils**).

- Il pacchetto **request-tracker4** è stato rimosso da trixie. È sostituito da **request-tracker5** che include istruzioni su come migrare i propri dati: si può mantenere installato il pacchetto **request-tracker4** ora obsoleto da bookworm durante la migrazione.
- I pacchetti **git-daemon-run** e **git-daemon-sysvinit** sono stati rimossi da trixie a causa di ragioni di sicurezza.
- I pacchetti **nvidia-graphics-drivers-tesla-470** non sono più supportati a monte e sono stati rimossi da trixie.
- Il pacchetto **deborphan** è stato rimosso da trixie. Per rimuovere i pacchetti non necessari si dovrebbe utilizzare `apt autoremove`, dopo `apt-mark minimize-manual`. Anche **debfoster** può essere uno strumento utile.
- Il pacchetto **tldr** è stato rimosso da trixie. Può essere sostituito con il pacchetto **tealdeer** o **tldr-py**.
- Il pacchetto **tpp** (Text Presentation Program) è stato rimosso da trixie. Può essere rimpiazzato con il pacchetto **lookatme** o **patat**.

5.3.2 Componenti deprecati per trixie

Con il prossimo rilascio di Debian 14 (nome in codice forky) alcune funzionalità diventeranno deprecate. Gli utenti dovranno migrare ad altre alternative per evitare problemi nell'aggiornamento a Debian 14.

Ciò include le seguenti funzionalità:

- Il pacchetto **sudo-ldap** verrà rimosso in forky. Il Team Debian di sudo ha deciso di abbandonare il suo uso a causa di difficoltà nella manutenzione e del suo uso limitato. I sistemi nuovi e quelli esistenti dovrebbero usare invece **libsss-sudo**.

  L'aggiornamento da trixie a forky senza che questa migrazione è stata completata può risultare in una perdita dell'atteso innalzamento di privilegi.

  Per ulteriori dettagli fare riferimento al bug n. 1033728 e al file NEWS nel pacchetto **sudo**.

- La funzionalità **sudo_logsrvd**, usata per il log dell'input/output di sudo, è possibile venga rimossa in Debian forky a meno che un manutentore non si faccia avanti. Questo comportamento ha un utilizzo limitato all'interno del contesto di Debian e mantenerlo aggiunge al pacchetto sudo di base una complessità non necessaria.

  Per discussioni in corso sull'argomento, vedere il bug n. 1101451 e il file NEWS nel pacchetto **sudo**.

- Il pacchetto **libnss-docker** non è più sviluppato a monte e richiede la versione 1.21 dell'API Docker. Quella versione deprecata dell'API è ancora supportata da Docker Engine v26 (fornito con Debian trixie), ma verrà rimossa in Docker Engine v27+ (fornito da Debian forky). A meno che lo sviluppo a monte non riprenda attività, il pacchetto verrà rimosso in Debian forky.

- I pacchetti **openssh-client** e **openssh-server** attualmente supportano l'autenticazione e lo scambio di chiavi GSS-API, che sono solitamente utilizzati per l'autenticazione su servizi Kerberos . Ciò ha causato alcuni problemi, specialmente sul lato server dove aggiunge nuove superfici per attacchi di pre-autenticazione e i pacchetti principali per OpenSSH in Debian smetteranno perciò di supportarlo a partire da forky.

  Se si sta usando l'autenticazione o lo scambio di chiavi GSS-API (cercare opzioni che iniziano con `GSSAPI` nei propri file di configurazione di OpenSSH) allora si dovrebbe installare subito il pacchetto **openssh-client-gssapi** (nei client) o **openssh-server-gssapi** (nei server). In trixie, questi sono pacchetti vuoti che dipendono da **openssh-client** e **openssh-server** rispettivamente; in forky, saranno creati separatamente.

- sbuild-debian-developer-setup è stato reso deprecato in favore di sbuild+unshare

  sbuild, lo strumento per compilare i pacchetti Debian in un ambiente minimale, ha ricevuto un aggiornamento importante e dovrebbe ora funzionare non appena installato. Per questo il pacchetto **sbuild-debian-developer-setup** non è più necessario ed è stato reso deprecato. Si può provare la nuova versione con:

```
$ sbuild --chroot-mode=unshare --dist=unstable hello
```

- Il pacchetto **fcitx** è stato reso deprecato in favore di **fcitx5**

  L'infrastruttura per metodo di input **fcitx**, nota anche come **fcitx4** o **fcitx 4.x**, non è più mantenuta a monte. Come risultato, tutti i pacchetti per metodo di input relativi sono ora deprecati. Il pacchetto **fcitx** e i pacchetti con nomi che iniziano con **fcitx-** verranno rimossi in Debian forky.

  Gli utenti attuali di **fcitx** sono incoraggiati a passare a **fcitx5** seguendo la guida alla migrazione degli autori originali di fcitx e la pagina del Wiki Debian.

- Il pacchetto per gestione di macchine virtuali **lxd** non viene più aggiornato e gli utenti dovrebbero passare all'uso di **incus**.

  Dopo che Canonical Ltd ha cambiato la licenza usata da LXD e ha introdotto un nuovo requisito di affidamento del copyright, è stato avviato il progetto Incus come fork mantenuto dalla comunità (vedere il bug n. 1058592). Debian raccomanda di passare da LXD a Incus. Il pacchetto **incus-extra** include strumenti per migrare i contenitori e le macchine virtuali da LXD.

- La suite **isc-dhcp** è deprecata dagli sviluppatori a monte.

  Se si sta usando **NetworkManager** o **systemd-networkd**, si può rimuovere senza problemi il pacchetto **isc-dhcp-client** dato che entrambi forniscono la propria implementazione. Se si sta usando il pacchetto **ifupdown**, **dhcpcd-base** fornisce un rimpiazzo. ISC raccomanda il pacchetto **Kea** come rimpiazzo per i server DHCP.

- Lo sviluppo di **KDE Frameworks 5** si è interrotto.

  I progetti KDE a monte hanno spostato i propri sforzi di sviluppo sulle librerie KDE Frameworks 6 basate su Qt 6 e quelle di KDE Frameworks 5 basate su Qt 5 non vengono più mantenute.

  Il Team Debian Qt / KDE ha in progetto di rimuovere KDE Frameworks 5 da Debian durante il ciclo di sviluppo di forky.

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 che sono stati etichettati come da ignorare nell'ultima parte del rilascio di trixie può essere trovata nel Sistema di tracciamento dei bug di (BTS). Al momento del rilascio, trixie era affetta dai seguenti bug degni di nota:

Numero di bug	Pacchetto (sorgente o binario)	Descrizione
1032240	**akonadi-backend-mysql**	akonadi server not robust aga
1078608	**apt**	apt update silently leaves old
1108467	**artha**	Segmentation fault
1109499	**bacula-director-sqlite3**	bacula-common: preinst inter
1108010	**src:e2fsprogs**	mc: error while loading share
1102690	**flash-kernel**	A higher version (...) is still
1109509	**gcc-offload-amdgcn**	fails to dist-upgrade from boo
1110119	**git-merge-changelog**	git-merge-changelog loses or
1036041	**src:grub2**	upgrade-reports: Dell XPS 9
1102160	**grub-efi-amd64**	upgrade-reports: Bookworm
913916	**grub-efi-amd64**	UEFI boot option removed af
984760	**grub-efi-amd64**	upgrade works, boot fails (err
1099655	**kmod**	initramfs-tools 146 generates
935182	**libreoffice-core**	Concurrent file open on the sa
1017906	**src:librsvg**	Contains generated files whos

Tabella 1 – continua dalla pagina precec

Numero di bug	Pacchetto (sorgente o binario)	Descrizione
1109203	**src:linux**	linux-image-6.12.35+deb13-a
1109512	**liblldb-dev**	fails to dist-upgrade from boo
1104231	**libmlir-17t64**	libmlir-17t64 is couninstallab
1084955	**src:llvm-toolchain-18**	llvm-toolchain-*: assembly c
1104177	**libc++-18-dev,libunwind-18-dev,libc++abi1-18,libc++abi-18-dev,libunwind-18**	libc++-18-dev fails to coinsta
1104336	**libmlir-18**	libmlir-18 is Multi-Arch: sam
1084954	**src:llvm-toolchain-19**	llvm-toolchain-*: assembly c
1095866	**llvm-19**	llvm-toolchain-19: unsoundn
1100981	**libmlir-19**	libmlir-19 fails to coinstall
1109519	**mbox-importer**	fails to dist-upgrade from boo
1110263	**openshot-qt**	does not start at all – Attribut
1108039	**python3.13**	An object referenced only thr
1089432	**src:shim**	Supporting rootless builds by
1101956	**snapd**	core18-based snap apps don't
1101839	**python3-tqdm**	segmentation fault in destruct
1017891	**src:vala**	Ships autogenerated files that
1109833	**voctomix-gui**	cannot import SafeConfigPars
988477	**src:xen**	xen-hypervisor-4.14-amd64:

CAPITOLO 6

Maggiori informazioni su Debian

6.1 Ulteriori letture

Oltre alle presenti note di rilascio e alla guida all'installazione (all'indirizzo https://www.debian.org/releases/trixie/installmanual), 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 web della documentazione Debian e il Wiki Debian.

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.

Per maggiori informazioni su OFTC visitare il sito web.

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.

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 si fornisce un contributo alla comunità. Identificare (e anche risolvere) problemi relativi allo sviluppo della distribuzione tramite la partecipazione alle liste per lo sviluppo è un'altra attività estremamente utile. Per mantenere l'alta qualità della distribuzione Debian si possono segnalare errori, 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 o a tradurre 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. Se si ha un interesse verso qualche area specifica, si potrebbe trovare piacevole fornire un contributo a qualcuno fra i sottoprogetti di Debian, che comprendono port verso architetture particolari e, fra i molti altri, Debian Pure Blends 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

Gestire il proprio sistema bookworm prima dell'avanzamento

Questa appendice contiene informazioni su come accertarsi di poter aggiornare o installare i pacchetti di bookworm prima di aggiornare a trixie.

7.1 Aggiornare il proprio sistema bookworm

In linea di principio non vi è alcuna differenza rispetto a qualsiasi altro aggiornamento effettuato in precedenza per bookworm. L'unica differenza è che dapprima sarà necessario accertarsi che il proprio elenco dei pacchetti contenga ancora i riferimenti a bookworm come illustrato in *Controllare i propri file source-list per APT*.

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

7.2 Controllare la propria configurazione di APT

Se qualsiasi riga nei propri file delle fonti di APT (vedere sources.list(5)) contiene riferimenti a «stable», in effetti sta già puntando a trixie. Ciò potrebbe non essere quello che si vuole se non si è ancora pronti per l'agg. 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 trixie, probabilmente non ha più molto senso installare pacchetti da bookworm. 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 o i file rilevanti delle fonti di APT (come ad esempio `/etc/apt/sources.list` o qualsiasi file in `/etc/apt/sources.list.d/`) con il proprio editor preferito e controllare tutte le righe che cominciano con

- `deb http:`
- `deb https:`
- `deb tor+http:`
- `deb tor+https:`

- `URIs: http:`
- `URIs: https:`
- `URIs: tor+http:`
- `URIs: tor+https:`

cercando un riferimento a «stable». Se ve n'è qualcuno, si cambi «stable» in «bookworm».

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 bookworm o di trixie.

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.

7.3 Effettuare l'aggiornamento al rilascio bookworm più recente

Per aggiornare tutti i pacchetti allo stato nel più recente rilascio minore di bookworm, eseguire

```
# apt full-upgrade
```

7.4 Rimuovere file di configurazione obsoleti

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

CAPITOLO 8

Contributori delle note di rilascio

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

- Adam D. Barrat (varie correzioni nel 2013),
- Adam Di Carlo (rilasci precedenti),
- Andreas Barth aba (rilasci precedenti: 2005 - 2007),
- Andrei Popescu (vari contributi),
- Anne Bezemer (rilascio precedente),
- Bob Hilliard (rilascio precedente),
- Charles Plessy (descrizione del problema GM965),
- Christian Perrier bubulle (Installazione di Lenny),
- Christoph Berg (Problemi specifici con PostgreSQL),
- Daniel Baumann (Debian Live),
- David Prévot taffit (rilascio di Wheezy),
- Eddy Petrișor (vari contributi),
- Emmanuel Kasper (backport),
- Esko Arajärvi (rifacimento dell'aggiornamento X11),
- Frans Pop fjp (rilascio precedente Etch),
- Giovanni Rapagnani (innumerevoli contributi),
- Gordon Farquharson (problemi del port ARM),
- Hideki Yamane henrich (ha contribuito e contribuisce dal 2006),
- Holger Wansing holgerw (ha contribuito e contribuisce dal 2009),
- Javier Fernández-Sanguino Peña jfs (rilascio di Etch, rilascio di Squeeze),
- Jens Seidel (Traduzione in tedesco, innumerevoli contributi),

- Jonas Meurer (problemi di syslog),
- Jonathan Nieder (rilascio di Squeeze, rilascio di Wheezy),
- Joost van Baal-Ilić joostvb (rilascio di Wheezy, rilascio di Jessie),
- Josip Rodin (rilasci precedenti),
- Julien Cristau jcristau (rilascio di Squeeze, rilascio di Wheezy),
- Justin B Rye (correzioni in inglese),
- LaMont Jones (descrizione dei problemi di NFS),
- Luk Claes (motivatore dei redattori),
- Martin Michlmayr (problemi del port ARM),
- Michael Biebl (problemi di syslog),
- Moritz Mühlenhoff (vari contributi),
- Niels Thykier nthykier (rilascio di Jessie),
- Noah Meyerhans (innumerevoli contributi),
- Noritada Kobayashi (traduzione in giapponese (coordinamento), innumerevoli contributi),
- Osamu Aoki (vari contributi),
- Paul Gevers elbrus (rilascio di Buster),
- Peter Green (nota relativa alla versione del kernel),
- Rob Bradford (rilascio di Etch),
- Samuel Thibault (descrizione del supporto per Braille),
- Simon Bienlein (descrizione del supporto per Braille),
- Simon Paillard spaillar-guest (innumerevoli contributi),
- Stefan Fritsch (descrizione dei problemi di Apache),
- Steve Langasek (rilascio di Etch),
- Steve McIntyre (Debian CDs),
- Tobias Scherer (descrizione di "proposed-update"),
- victory victory-guest (correzioni dei markup, ha contribuito e contribuisce dal 2006),
- Vincent McIntyre (descrizione di "proposed-update"),
- W. Martin Borgert (modifiche alle note di rilascio di Lenny e passaggio a DocBook XML).

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