Note di rilascio per Debian 10 (buster), PC a 64 bit

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

3 luglio 2022

Indice

Capitolo 1

Introduzione

Questo documento fornisce informazioni agli utenti della distribuzione Debian sui cambiamenti principali nella versione 10 (nome in codice buster).

Le note di rilascio forniscono informazioni su come aggiornare in modo sicuro dalla versione 9 (nome in codice stretch) 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/buster/releasenotes`. Nel dubbio, controllare la data del documento nel frontespizio e assicurarsi di avere l'ultima versione disponibile.

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 stretch). 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 stretch.

1.1 Segnalare errori in questo documento

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

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

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

1.2 Fornire resoconti di aggiornamento

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

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

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

NOTA

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

1.3 Sorgenti di questo documento

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

Capitolo 2

Cosa c'è di nuovo in Debian 10

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

2.1 Architetture supportate

Le seguenti architetture sono ufficialmente supportate da Debian 10:

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

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

2.2 Cosa c'è di nuovo nella distribuzione?

Ancora una volta la nuova versione di Debian contiene molto più software rispetto alla precedente, stretch; la distribuzione include più di 13370 nuovi pacchetti, per un totale di oltre 57703 pacchetti. La maggior parte del software nella distribuzione è stata aggiornata: più di 35532 pacchetti software (corrispondenti al 62% di tutti i pacchetti in stretch). Inoltre, un notevole numero di pacchetti (oltre 7278, il 13% dei pacchetti in stretch) è stato rimosso dalla distribuzione per diversi motivi. Non ci saranno aggiornamenti per questi pacchetti ed essi saranno marcati come «obsoleti» nelle interfacce dei programmi di gestione dei pacchetti; vedere Sezione 4.8.

Debian viene ancora una volta fornita con molti ambienti e applicazioni desktop. Fra l'altro include ora gli ambienti desktop GNOME 3.30, KDE Plasma 5.14, LXDE 10, LXQt 0.14, MATE 1.20 e Xfce 4.12.

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

- LibreOffice viene aggiornato alla versione 6.1;
- Calligra viene aggiornato a 3.1.
- GNUcash viene aggiornato a 3.4;

Con buster Debian per la prima volta fornisce un'infrastruttura di controllo degli accessi obbligatorio abilitata in modo predefinito. Le nuove installazioni di Debian buster avranno installato AppArmor che sarà abilitato in modo predefinito. Vedere più avanti per ulteriori informazioni.

Inoltre buster è il primo rilascio Debian ad essere fornito con programmi basati su Rust come Firefox, ripgrep, fd, exa, ecc. e un significativo numero di librerie basate su Rust (più di 450). Buster viene fornito con Rustc 1.34.

Tra gli aggiornamenti di altre applicazioni per il desktop è incluso l'aggiornamento di Evolution a 3.30.

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

Pacchetto	**Versione in 9 (stretch)**	**Versione in 10 (buster)**
Apache	2.4.25	2.4.38
BIND Server DNS	9.10	9.11
Cryptsetup	1.7	2.1
Dovecot MTA	2.2.27	2.3.4
Emacs	24.5 e 25.1	26.1
Exim, server predefinito per la posta elettronica	4.89	4.92
GNU Compiler Collection come compilatore predefinito	6.3	7.4 e 8.3
GIMP	2.8.18	2.10.8
GnuPG	2.1	2.2
Inkscape	0.92.1	0.92.4
la libreria C GNU	2.24	2.28
lighttpd	1.4.45	1.4.53
Immagine del kernel Linux	serie 4.9	serie 4.19
Insieme di strumenti LLVM/-Clang	3.7	6.0.1 e 7.0.1 (predefinito)
MariaDB	10.1	10.3
Nginx	1.10	1.14
OpenJDK	8	11
OpenSSH	7.4p1	7.9p1
Perl	5.24	5.28
PHP	7.0	7.3
MTA Postfix	3.1.8	3.3.2
PostgreSQL	9.6	11
Python 3	3.5.3	3.7.3
Rustc		1.34
Samba	4.5	4.9
Vim	8.0	8.1

2.2.1 UEFI Secure Boot

Il Secure Boot è una funzionalità abilitata nella maggior parte dei PC che evita che venga caricato codice non firmato, proteggendo da alcuni tipi di bootkit e rootkit.

Debian può ora essere installata ed eseguita sulla maggior parte dei PC con abilitato il Secure Boot

È possibile abilitare il Secure Boot in un sistema che ha una installazione di Debian esistente, se fa già l'avvio usando UEFI. Prima di farlo è necessario installare `shim-signed`, `grub-efi-amd64-signed` o `grub-efi-ia32-signed` e un pacchetto del kernel Linux da buster.

Alcune funzionalità di GRUB e Linux sono limitate con la modalità Secure Boot, per evitare modifiche del loro codice.

Ulteriori informazioni si possono trovare sul wiki Debian alla pagina SecureBoot (`https://wiki.debian.org/SecureBoot`).

2.2.2 AppArmor abilitato in modo predefinito

Debian buster ha `AppArmor` abilitato in modo predefinito. `AppArmor` è un'infrastruttura di controllo degli accessi obbligatorio per limitare le capacità dei programmi (come permessi di montaggio, ptrace

e segnali, o accesso a file in lettura, scrittura ed esecuzione) definendo profili per ciascun programma.

Il pacchetto `apparmor` viene fornito con profili AppArmor per svariati programmi. Alcuni altri pacchetti, come `evince`, includono profili per i programmi che forniscono. Ulteriori profili possono essere trovati nel pacchetto `apparmor-profiles-extra`.

`AppArmor` viene richiamato per l'installazione a causa di una voce `Recommends` (Raccomanda) del pacchetto del kernel Linux di buster. Nei sistemi che sono configurati per non installare in modo predefinito i pacchetti raccomandati, il pacchetto `apparmor` può essere installato manualmente per abilitare `AppArmor`.

2.2.3 Hardening opzionale di APT

Tutti i metodi forniti da APT (es. http e https), tranne cdrom, gpgv e rsh, possono fare uso delle sandbox seccomp-BPF come fornite dal kernel Linux, per restringere la lista delle chiamate di sistema permesse e intrappolare tutte le altre con un segnale `SIGSYS`. Questo uso delle sandbox è attualmente attivo solo se lo si attiva appositamente e deve essere abilitato con:

```
APT::Sandbox::Seccomp che è un valore booleano per attivarlo/disattivarlo
```

Due opzioni possono essere utilizzate per configurarlo ulteriormente:

```
APT::Sandbox::Seccomp::Trap è un elenco di nomi di altre chiamate di ↩
    sistema da intrappolare
APT::Sandbox::Seccomp::Allow è un elenco di nomi di altre chiamate di ↩
    sistema da permettere
```

2.2.4 Aggiornamenti non presidiati ("unattended-upgrades") per rilasci minori di stable

Le versioni precedenti di `unattended-upgrades` in modo predefinito installavano solo gli aggiornamenti provenienti dalla suite di sicurezza. In buster ora aggiorna automaticamente al rilascio minore di stable più recente. Per i dettagli vedere il file NEWS.Debian del pacchetto.

2.2.5 Pagine di manuale sostanzialmente migliorate per gli utenti di lingua tedesca

La documentazione (pagine `man`) per svariati progetti come `systemd`, `util-linux` e `mutt` è stata sostanzialmente ampliata. Installare `manpages-de` per sfruttare i miglioramenti. Durante la vita di buster verranno forniti ulteriori miglioramenti / traduzioni all'interno dell'archivio `backports`.

2.2.6 Filtraggio di rete basato in modo predefinito sull'infrastruttura nftables

A partire da `iptables` v1.8.2 il pacchetto binario include `iptables-nft` e `iptables-legacy`, due varianti dell'interfaccia a riga di comando di `iptables`. La variante basata su nftables, che usa il sottosistema `nf_tables` del kernel Linux, è quella predefinita in buster. Quella vecchia usa il sottosistema `x_tables` del kernel Linux. Il sistema `update-alternatives` può essere utilizzato per selezionare una variante o l'altra.

Ciò è vero per tutte gli strumenti e le utilità correlate:

- iptables
- iptables-save
- iptables-restore
- ip6tables
- ip6tables-save
- ip6tables-restore

- arptables
- arptables-save
- arptables-restore
- ebtables
- ebtables-save
- ebtables-restore

Anche tutti questi hanno acquisito le varianti `-nft` e `-legacy`. L'opzione `-nft` è per gli utenti che non possono, o non desiderano, migrare all'interfaccia a riga di comando nativa `nftables`. Tuttavia gli utenti sono fortemente incoraggiati a passare all'interfaccia `nftables` invece di usare la vecchia interfaccia `iptables`.

`nftables` fornisce un rimpiazzo completo per `iptables` con prestazioni molto migliori, una sintassi rinnovata, migliore supporto per firewall IPv4/IPv6 dual-stack, operazioni completamente atomiche per aggiornamenti dinamici dell'insieme di regole, un'API Netlink per applicazioni di terze parti, classificazione dei pacchetti più veloce attraverso infrastrutture generiche migliorate per insiemi e mappe e molti altri miglioramenti (`https://wiki.nftables.org`).

Questo cambiamento è in linea con ciò che stanno facendo altre popolari distribuzioni Linux, come RedHat, che ora usa `nftables` come suo strumento predefinito per firewall (`https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8-beta/html-single/8.0_beta_release_notes/index#networking_2`).

Inoltre, è da notare che tutti i binari `iptables` sono ora installati in `/usr/sbin` invece di `/sbin`. Viene creato un collegamento simbolico di compatibilità, ma verrà abbandonato dopo il ciclo di rilascio di buster. I percorsi di binari specificati in maniera fissa in script dovranno essere corretti ed è meglio evitarli.

Una documentazione esaustiva è disponibile nei file README e NEWS del pacchetto e nel Wiki Debian (`https://wiki.debian.org/nftables`).

2.2.7 Cryptsetup usa in modo predefinito il formato LUKS2 su disco

La versione di `cryptsetup` fornita con Debian buster usa il nuovo formato su disco `LUKS2`. I nuovi volumi `LUKS` useranno in modo predefinito tale formato.

A differenza del precedente formato `LUKS1`, `LUKS2` fornisce ridondanza dei metadati, rilevazione di corruzione dei metadati e algoritmi `PBKDF` configurabili. Anche la cifratura autenticata è gestita, ma marcata ancora come sperimentale.

I volumi `LUKS1` esistenti non saranno aggiornati automaticamente. Possono essere convertiti ma non tutte le funzionalità di `LUKS2` saranno disponibili a causa di incompatibilità nella dimensione delle intestazioni. Vedere la pagina di manuale di cryptsetup (`https://manpages.debian.org/buster/cryptsetup`) per maggiori informazioni.

Notare che il bootloader GNU GRUB non gestisce ancora il formato . Vedere la documentazione (`https://cryptsetup-team.pages.debian.net/cryptsetup/encrypted-boot.html`) corrispondente per ulteriori informazioni su come installare Debian 10 con boot cifrato.

2.2.8 Stampa senza driver con CUPS 2.2.10

Debian 10 fornisce CUPS 2.2.10 e `cups-filters` 1.21.6. Insieme forniscono all'utente tutto ciò di cui ha bisogno per sfruttare la stampa senza driver (`https://wiki.debian.org/DriverlessPrinting`). Il requisito principale è che la coda di stampa di rete o la stampante offra un servizio AirPrint. Una stampante IPP moderna molto probabilmente è compatibile con AirPrint; una coda di stampa CUPS di Debian è sempre compatibile con AirPrint.

In sostanza il DNS-SD (Bonjour) fa il broadcasting da un server CUPS pubblicizzando una coda o quelle da stampanti IPP sono in grado di essere visualizzate nei dialoghi di stampa delle applicazioni senza che sia necessaria alcuna azione da parte dell'utente. Un beneficio aggiuntivo è che ci si può disfare dell'uso di driver di stampa e plugin non liberi dei produttori.

Un'installazione predefinita del pacchetto `cups` installa anche il pacchetto `cups-browsed`; le code di stampa e le stampanti IPP saranno così automaticamente impostate e gestite da questa utilità. Questo è il modo raccomandato (`https://wiki.debian.org/QuickPrintQueuesCUPS`) agli utenti per avere un'esperienza di stampa senza driver che sia diretta e senza problemi.

2.2.9 Supporto di base per i dispositivi basati su Allwinner A64

Grazie agli sforzi della comunità linux-sunxi (`https://linux-sunxi.org`), Debian buster ha un supporto di base per molti dispositivi basati sul SoC Allwinner A64. Ciò include FriendlyARM NanoPi A64; Olimex A64-OLinuXino e TERES-A64, PINE64 PINE A64/A64+/A64-LTS, SOPINE e Pinebook; SINOVOIP Banana Pi BPI-M64; e Xunlong Orange Pi Win (Plus).

Le funzionalità essenziali di questi dispositivi (es. console seriale, ethernet, porte USB e output video di base) dovrebbero funzionare con il kernel di buster. Ulteriori funzionalità avanzate (es. audio o accelerazione video) sono incluse o ne è programmata l'inclusione in kernel successivi che saranno resi disponibili come di consueto attraverso l'archivio dei backport (`https://backports.debian.org`). Vedere anche la pagina di stato (`https://linux-sunxi.org/Linux_mainlining_effort`) per lo sforzo di mainlining di Linux.

2.2.10 Novità dal Blend Debian Med

Il team Debian Med ha aggiunto svariati nuovi pacchetti e aggiornamenti per il software mirato alle scienze naturali e alla medicina. È proseguito e proseguirà lo sforzo per aggiungere il supporto per l'integrazione continua (Continuous Integration) per i pacchetti in questo campo.

Per installare i pacchetti mantenuti dal team Debian Med, installare i metapacchetti chiamati `med-*` che sono alla versione 3.3 per Debian buster. Visitare le pagine delle attività Debian Med (`http://blends.debian.org/med/tasks`) per vedere l'intera gamma del software per biologia e medicina disponibile in Debian.

2.2.11 GNOME usa in modo predefinito Wayland

Seguendo gli autori originali, in buster GNOME usa in modo predefinito il server di display Wayland invece di Xorg. Wayland ha un disegno progettuale più semplice e moderno, che ha vantaggi dal punto di vista della sicurezza.

Il server di display Xorg è ancora installato in modo predefinito e il gestore di display predefinito permette comunque di sceglierlo come server di display per la sessione successiva, e ciò potrebbe essere necessario se si desiderano usare alcune applicazioni (vedere Sezione 5.1.9).

A coloro che richiedono funzionalità di accessibilità per il server di display, ad esempio scorciatoie da tastiera globali, è raccomandato l'uso di Xorg invece di Wayland.

2.2.12 /usr unificata nelle nuove installazioni

Nelle nuove installazioni, il contenuto di `/bin`, `/sbin` e `/lib` viene installato in modo predefinito nelle loro controparti `/usr`. `/bin`, `/sbin` e `/lib` sono collegamenti simbolici che puntano alle rispettive directory controparti in `/usr/`. In forma grafica:

```
/bin → /usr/bin
/sbin → /usr/sbin
/lib → /usr/lib
```

Quando si aggiorna a buster, i sistemi vengono lasciati come sono, anche se esiste il pacchetto `usrmerge` per fare la conversione, se lo si desidera. Il progetto freedesktop.org (`https://www.freedesktop.org`) ospita un Wiki (`https://www.freedesktop.org/wiki/Software/systemd/TheCaseForTheUsrMerg` con spiegate gran parti delle motivazioni.

Questo cambiamento non dovrebbe avere effetti per gli utenti normali che eseguono solo i pacchetti forniti da Debian, ma può essere una cosa di cui deve essere informato chi usa o compila software di terze parti.

2.2.13 Novità dal Team Debian Live

Il team Debian Live è orgoglioso di introdurre le ISO live con LXQt come nuova tipologia. LXQt è un ambiente desktop Qt leggero. Non è invadente. Non si blocca o rallenta il sistema. Si focalizza sull'essere un desktop classico con un aspetto e stile moderni.

L'ambiente desktop LXQt offerto dal progetto Debian Live LXQt è puro, non modificati, perciò si ottiene l'esperienza desktop standard che gli sviluppatori di LXQt hanno creato per il loro popolare

sistema operativo. Agli utenti viene presentata una disposizione LXQt standard formata da un singolo pannello (barra delle attività) posizionata all'estremità in basso dello schermo che include varie applet utili, come il menu principale, il gestore delle attività, l'avviatore delle applicazioni, l'area del vassoio di sistema e il calendario integrato.

Le immagini live di buster sono fornite con qualcosa di nuovo che è stato adottato anche da moltissime altre distribuzioni, cioè l'installatore Calamares. Calamares è un progetto di installatore indipendente (viene chiamato «L'infrastruttura universale per installatore»? che offre un'interfaccia basata su Qt per installare un sistema. Non sostituisce l'installatore Debian nelle immagini live; piuttosto è per un pubblico diverso.

Calamares è veramente facile da usare, con partizionamento guidato facile e un'impostazione veramente semplice della cifratura dell'intero disco. Non copre tutte le funzionalità avanzate dell'installatore Debian (anche se ha proprio di recente aggiunto il supporto per RAID) né ha una modalità di installazione non presidiata. Tuttavia per più del 95% degli utenti di desktop e portatili, Calamares è un modo molto più semplice di installare un sistema, il che lo rende molto adatto ai sistemi live. Per tutti coloro che necessitano di qualcosa di più complicato, o che devono fare un'installazione in massa, l'installatore Debian è sempre disponibile in forma sia testuale sia con GUI.

Debian Live Buster reintroduce l'immagine live standard. Questa è un'immagine Debian di base che contiene un sistema Debian di base, senza alcuna interfaccia utente grafica. Dato che installa da un'immagine squashfs, invece di installare i file di sistema usando **dpkg**, i tempi di installazione sono molto più veloci rispetto ad installare da un'immagine di installazione Debian minimale.

Capitolo 3

Sistema d'installazione

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

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

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

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

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

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

L'installatore Debian ha fatto molti passi avanti dalla precedente versione rilasciata ufficialmente con Debian 9, raggiungendo un migliore supporto all'hardware e alcune nuove e interessanti funzionalità e migliorie.

In particolare c'è il supporto iniziale per l'UEFI Secure Boot (vedere Sezione 2.2.1) che è stato aggiunto alle immagini di installazione.

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

3.1.1 Installazione automatizzata

Alcuni cambiamenti menzionati nella sezione precedente implicano anche modifiche al supporto nell'installatore per installazioni automatizzate con l'uso di file di preconfigurazione. Ciò significa che se si possiedono file preconfigurati che funzionavano con l'installatore di stretch non ci si può attendere che questi funzionino anche con la nuova versione senza modifiche.

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

Capitolo 4

Aggiornamenti da Debian 9 (stretch)

4.1 Preparazione all'aggiornamento

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

4.1.1 Salvare i dati e le informazioni di configurazione

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

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

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

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

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

4.1.2 Informare gli utenti in anticipo

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

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

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

4.1.3 Preparazione all'indisponibilità dei servizi

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

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

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

4.1.4 Preparazione per il ripristino

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

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

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

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

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

4.1.4.1 Shell di debug durante l'avvio con initrd

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

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

Se si è riusciti a risolvere il problema, digitando `exit` si uscirà dalla shell di debug e si continuerà il processo di avvio a partire dal punto in cui il problema si è verificato. Naturalmente sarà anche necessario risolvere il problema sottostante e rigenerare initrd in modo che il prossimo avvio non fallisca nuovamente.

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

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

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

4.1.4.2 Shell di debug durante l'avvio con systemd

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

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

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

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

4.1.5 Preparazione di un ambiente sicuro per l'aggiornamento

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

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

4.1.6 Verificare il supporto per i nomi delle interfacce di rete

I sistemi aggiornati da rilasci più vecchi che usano ancora interfacce di rete con nomi come `eth0` o `wlan0` rischiano di perdere la rete una volta passati a buster; vedere Sezione 5.1.6 per istruzioni sulla migrazione.

4.2 Verificare lo stato di configurazione di APT

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

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

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

```
$ aptitude search '~i(!~ODebian)'
$ apt-forktracer | sort
```

L'aggiornamento diretto dalle versioni di Debian precedenti a 9 (stretch) non è supportato. Seguire le istruzioni nelle Note di rilascio per Debian 9 (`https://www.debian.org/releases/stretch/releasenotes`) per aggiornare prima a Debian 9.

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

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

È una buona idea rimuovere i pacchetti obsoleti dal proprio sistema prima dell'aggiornamento.

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

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

4.2.2 Fonti non ufficiali

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

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

4.2.3 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).

4.2.4 Verifica dello stato dei pacchetti

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

```
# dpkg --audit
```

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

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

o

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

[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.

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

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

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

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

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

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

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

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

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

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

4.3 Preparazione dei file source-list per APT

Prima di iniziare l'aggiornamento è necessario riconfigurare i file source-list di APT (`/etc/apt/sources.list` e i file in `/etc/apt/sources.list.d/`).

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

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

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

4.3.1 Aggiunta di fonti internet per APT

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

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

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

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

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

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

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

```
    http://mirrors.kernel.org/debian/dists/buster/main/binary-amd64/...
    http://mirrors.kernel.org/debian/dists/buster/contrib/binary-amd64/...
```

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

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

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

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

4.3.2 Aggiunta di fonti per APT da mirror locale

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

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

```
    /var/local/debian/dists/buster/main/binary-amd64/...
    /var/local/debian/dists/buster/contrib/binary-amd64/...
```

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

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

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

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

4.3.3 Aggiunta di fonti per APT da supporti ottici

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

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

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

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

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

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

Poi, si esegua:

```
# apt-cdrom add
```

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

4.4 Aggiornare i pacchetti

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

NOTA

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

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

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

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

NOTA

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

4.4.1 Registrazione della sessione

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

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

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

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

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

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

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

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

4.4.2 Aggiornamento della lista dei pacchetti

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

```
# apt update
```

NOTA

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

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

Prima di aggiornare il proprio sistema ci si deve accertare di avere uno spazio disponibile sufficiente sul proprio disco fisso al momento di far partire l'aggiornamento completo del sistema, come descritto in Sezione 4.4.5. Per prima cosa, poiché ogni pacchetto necessario per l'installazione prelevato dalla rete è immagazzinato in `/var/cache/apt/archives` (e nella sottodirectory `partial/`, durante lo scaricamento), ci si dovrebbe assicurare di avere spazio a sufficienza nella partizione del file system che contiene `/var` per il temporaneo scaricamento dei pacchetti che saranno installati nel sistema. Dopo lo scaricamento sarà probabilmente necessario avere ulteriore spazio disponibile in altre partizioni del file system per poter installare sia i pacchetti aggiornati (che potrebbero contenere file binari più grossi o più dati), sia i nuovi pacchetti che saranno introdotti con l'aggiornamento. Se il sistema non ha spazio libero a sufficienza, si potrebbe finire con un aggiornamento incompleto dal quale è difficile effettuare un ripristino.

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

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

NOTA

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

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

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

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

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

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

  ```
  # apt autoremove
  ```

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

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

- Eliminare i file di traduzioni e localizzazioni dal sistema se non sono necessari. È possibile installare il pacchetto `localepurge` e configurarlo in modo che solo poche localizzazioni selezionate vengano mantenute sul sistema. Questo ridurrà lo spazio su disco occupato da `/usr/share/locale`.

- Spostare temporaneamente su un altro sistema o rimuovere in modo permanente i log di sistema che si trovano in `/var/log`.

- Usare un `/var/cache/apt/archives` temporaneo: è possibile usare una directory di cache temporanea da un altro file system (periferiche di memorizzazione USB, dischi fissi temporanei, file system già in uso, ecc.).

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

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

1. si rimuovano i pacchetti precedentemente scaricati per l'installazione:

```
# apt clean
```

2. si copi la directory `/var/cache/apt/archives` nella periferica USB:

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

3. si monti la directory della cache temporanea su quella attuale:

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

4. dopo l'aggiornamento, si ripristini la directory `/var/cache/apt/archives` originale:

```
# umount /media/usbkey/archives
```

5. si rimuova il restante `/media/usbkey/archives`.

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

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

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

4.4.4 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 Sezione 4.4.5.

Per farlo eseguire:

```
# apt-get upgrade
```

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

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

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

4.4.5 Aggiornamento del sistema

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

```
# apt full-upgrade
```

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

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

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

4.5 Possibili problemi durante l'aggiornamento

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

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

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

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

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

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

4.5.2 Rimozioni attese

Il processo d'aggiornamento a buster 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 buster vedere Sezione 4.8.

4.5.3 Conflitti e pre-dipendenze cicliche

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

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

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

per eliminare alcuni dei pacchetti che generano il problema, o

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

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

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

4.5.4 Conflitti tra file

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

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

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

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

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

4.5.5 Modifiche alla configurazione

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

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

4.5.6 Cambiare la sessione sulla console

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

Per recuperare la console su cui era in corso l'aggiornamento, usare Ctrl + Alt + F1, se si è nella schermata di avvio grafico, oppure usare Alt + F1 se si è in una console testuale locale, per tornare al terminale virtuale 1. Al posto di F1 usare il tasto funzione con lo stesso numero del terminale virtuale su cui era in corso l'aggiornamento. Per scorrere i diversi terminali in modalità testuale è possibile usare Alt + Freccia sinistra o Alt + Freccia destra.

4.6 Aggiornare il kernel e i pacchetti collegati

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

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

4.6.1 Installazione di un metapacchetto del kernel

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

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

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

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

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

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

Si dovrebbe quindi utilizzare `apt install` per installarlo. Una volta che questo nuovo kernel è installato si dovrebbe riavviare alla prossima opportunità disponibile per poter godere dei benefici offerti dalla nuova versione del kernel. Tuttavia guardare Sezione 5.1.12 prima di effettuare il primo riavvio dopo l'aggiornamento.

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

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

4.7 Preparazione per il prossimo rilascio

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

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

4.7.1 Eliminare completamente i pacchetti rimossi

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

ATTENZIONE

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

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

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

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

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

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

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

4.8 Pacchetti obsoleti

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

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

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

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

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

ftp.debian.org (`https://bugs.debian.org/cgi-bin/pkgreport.cgi?pkg=ftp.debian.org&archive=yes`).

Per un elenco dei pacchetto obsoleti per Buster fare riferimento a Sezione 5.1.10.

4.8.1 Pacchetti fittizi di transizione

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

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

Capitolo 5

Problemi di cui essere al corrente per buster

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

5.1 Aspetti specifici dell'aggiornamento a buster

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

5.1.1 Opzione di mount hidepid per procfs non supportata

È noto che l'opzione di montaggio `hidepid` per `/proc` causa problemi con l'attuale versione di systemd ed è considerata dagli autori originali di systemd come una configurazione non supportata. Agli utenti che hanno modificato `/etc/fstab` per abilitare questa opzione viene suggerito di disabilitarla prima dell'aggiornamento, per assicurare che le sessioni di login funzionino su buster. (Una possibile soluzione per riabilitarla è descritta nella pagina Hardening (`https://wiki.debian.org/Hardening#Mounting_.2Fproc_with_hidepid`) del wiki.)

5.1.2 l'avvio di upbind fallisce con -no-dbus

Le opzioni predefinite di `ypbind` sono cambiate. Tuttavia, se questo file è stato modificato i vecchi valori predefiniti non verranno aggiornati e ci si deve accertare che l'opzione `YPBINDARGS=` in `/etc/default/nis` non `includa -no-dbus`. Se `-no-dbus` è presente l'avvio di **ypbind** fallirà e potrebbe non essere possibile fare il login. Per maggiori informazioni vedere il bug n.906436 (`https://bugs.debian.org/906436`).

5.1.3 NIS server does not answer NIS client requests by default

The default behavior of `rpcbind` has changed to no longer answer remote calls from NIS clients. On NIS servers you will need to add the (Debian-specific) `-r` flag to the command line options of **rpcbind**, otherwise users will not be able to log into your NIS client machines. For more info see bug #935492 (`https://bugs.debian.org/935492`).

5.1.4 sshd fallisce l'autenticazione

La semantica di `PubkeyAcceptedKeyTypes` e delle opzioni simili `HostbasedAcceptedKeyTypes` per `sshd` è cambiata. Ora specificano algoritmi di firma che sono accettati per i rispettivi meccanismi di autenticazione, mentre prima specificavano i tipi di chiave accettati. Questa distinzione è importante quando si usano algoritmi di firma RSA/SHA2 `rsa-sha2-256`, `rsa-sha2-512` e le loro controparti

certificato. Le configurazioni che sovrascrivono queste opzioni, ma omettono questi nomi di algoritmi possono causare fallimenti inattesi delle autenticazioni.

Non è necessaria alcuna azione per le configurazioni che accettano i valori predefiniti per queste opzioni.

5.1.5 Fallisce l'avvio dei demoni o il sistema sembra bloccato durante l'avvio

Poiché `systemd` ha bisogno di entropia durante l'avvio e il kernel tratta tali chiamate come bloccanti quando l'entropia disponibile è poca, il sistema può bloccarsi per un tempo da qualche minuto fino ad ore fino a che il sottosistema della casualità è sufficientemente inizializzato (`random: crng init done`). Per i sistemi `amd64` con supporto per l'istruzione `RDRAND` questo problema viene evitato dal kernel Debian che usa tale istruzione in modo predefinito (`CONFIG_RANDOM_TRUST_CPU`).

I sistemi non `amd64` e alcuni tipi di macchine virtuali devono fornire una fonte diversa di entropia per continuare l'avvio velocemente. `haveged` è stato scelto a questo scopo all'interno del progetto dell'Installatore Debian e può essere una valida opzione se l'entropia hardwae non è disponibile sul sistema. Nelle macchine virtuali considerare l'inoltro dell'entropia dall'host alle VM attraverso `virtio_rng`.

Se si legge questo documento dopo aver fatto l'aggiornamento di un sistema remoto a buster, fare ping al sistema in rete continuamente dato che ciò aggiunge entropia al pool della casualità e il sistema diventerà da ultimo nuovamente raggiungibile via ssh.

Vedere il wiki (`https://wiki.debian.org/BoottimeEntropyStarvation`) e la panoramica di DLange sul problema (`https://daniel-lange.com/archives/152-hello-buster.html`) per altre opzioni.

5.1.6 Migrazione dai sorpassati nomi delle interfacce di rete

Se il proprio sistema è stato aggiornato da un rilascio precedente e usa ancora i nomi delle interfacce di rete vecchio stile che sono stati deprecati a partire da stretch (come `eth0` o `wlan0`) si dovrebbe tenere a mente che il meccanismo di definizione dei loro nomi attraverso `/etc/udev/rules.d/70-persistent-net.rules` non è più ufficialmente supportato da `udev` in buster (sebbene possa ancora funzionare in alcuni casi). Per evitare il pericolo che la macchina perda la connettività di rete dopo l'aggiornamento a buster, è raccomandata la migrazione in anticipo al nuovo schema di nomi (solitamente ciò significa nomi come `enp0s1` o `wlp2s5` che incorporano bus PCI e numeri di slot). Assicurarsi di aggiornare ogni nome di interfaccia codificato in modo fisso nella configurazione per firewall, `ifupdown` e così via.

L'alternativa è passare ad un meccanismo supportato per forzare il vecchio schema dei nomi, come un file `.link` di systemd (vedere systemd.link(5) (`https://manpages.debian.org/buster/systemd.link`)). Anche l'opzione `net.ifnames=0` per la riga di comando del kernel potrebbe funzionare per i sistemi che hanno una sola interfaccia di rete (per ciascun tipo).

Per trovare i nomi nel nuovo stile che saranno utilizzati, trovare prima i nomi attuali delle interfacce interessate:

```
$ echo /sys/class/net/[ew]*
```

Per ciascuno di questi nomi controllare se è utilizzato in file di configurazione e quale nome `udev` preferirebbe usare per esso:

```
$ sudo rgrep -w eth0 /etc
$ udevadm test-builtin net_id /sys/class/net/eth0 2>/dev/null
```

Ciò dovrebbe fornire abbastanza informazioni per definire un piano di migrazione. (Se l'output di `udevadm` include un nome «onboard» o «slot», esso ha la precedenza; i nomi basati su MAC sono normalmente trattati come ripiego, ma possono essere necessari per l'hardware di rete USB.)

Una volta che si è pronti a fare il passaggio, disabilitare `70-persistent-net.rules` rinominandolo o commentando le singole righe. Nelle macchine virtuali è necessario rimuovere i file `/etc/systemd/network/99-default.link` e (se si usano devide di rete virtio) `/etc/systemd/network/50-virtio-kernel-names.link`. Poi ricreare il file `initrd`:

```
$ sudo update-initramfs -u
```

e riavviare. Il sistema dovrebbe avere ora i nomi di interfacce di rete nel nuovo stile. Aggiustare ogni file di configurazione rimanente e testare il sistema.

Vedere il wiki (`https://wiki.debian.org/NetworkInterfaceNames`), la documentazione originale a monte (`https://www.freedesktop.org/software/systemd/man/systemd.net-naming-sche` `html`) e il `README.Debian` di `udev` per maggiori informazioni.

5.1.7 Configurazione dei moduli per interfacce fittizie e di bonding

I sistemi che usano interfacce fittizie (”dummy”) e/o bonding dei canali per esempio per configurare una macchina come router, possono incontrare problemi nell'aggiornamento a buster. Le nuove versioni di `systemd` installano un file `/lib/modprobe.d/systemd.conf` (pensato per semplificare la configurazione attraverso **systemd-networkd**) contenente le righe

```
options bonding max_bonds=0
options dummy numdummies=0
```

Gli amministratori che dipendo da valori diversi devono assicurarsi di averli impostati in modo corretto in modo che abbiano la precedenza. Un file in `/etc/modprobe.d` scavalcherà uno con lo stesso nome in `/lib/modprobe.d`, ma i nomi sono elaborati in ordine alfabetico, perciò `/lib/modprobe.d/systemd.conf` segue e sovrascrive le impostazioni (ad esempio) di `/etc/modprobe.d/dummy.conf`. Assicurarsi che qualsiasi file locale abbia un nome che viene ordinato dopo «`systemd.conf`», come «`/etc/modprobe.d/zz-local.conf`».

5.1.8 Versione predefinita e livello di sicurezza di OpenSSL aumentati

Seguendo diverse raccomandazioni di sicurezza la versione minima predefinita di TLS è stata modificata da TLSv1 a TLSv1.2.

Anche il livello di sicurezza predefinito per le connessioni TLS è stato aumentato dal livello 1 al 2. Ciò sposta dal livello di sicurezza a 80 bit a quello a 112 bit e richiede chiavi RSA e DHE a minimo 2048, chiavi ECC a minimo 224 bit e SHA-2.

Le impostazioni a livello di sistema possono essere modificate in `/etc/ssl/openssl.cnf`. Inoltre le applicazioni possono avere un modo specifico per ciascuna applicazione di scavalcare i valori predefiniti.

Nel file `/etc/ssl/openssl.cnf` predefinito è presente una riga `MinProtocol` e una `CipherString`. `CipherString` può anche impostare il livello di sicurezza. Informazioni sui livelli di sicurezza possono essere trovate nella magina di manuale SSL_CTX_set_security_level(3ssl) (`https://manpages.debian.org/buster/SSL_CTX_set_security_level(3ssl)`). L'elenco delle stringhe valide per la versione minima del protocollo può essere trovato in SSL_CONF_cmd(3ssl) (`https://manpages.debian.org/buster/SSL_CONF_cmd(3ssl)`). Ulteriori informazioni possono essere trovate in ciphers(1ssl) (`https://manpages.debian.org/buster/ciphers(1ssl)`) e config(5ssl) (`https://manpages.debian.org/buster/config(5ssl)`).

Si possono modificare i valori predefiniti a livello di sistema in `/etc/ssl/openssl.cnf` ai loro valori precedenti impostando:

```
        MinProtocol = None
        CipherString = DEFAULT
```

È raccomandato contattare il sito remoto se i valori predefiniti causano problemi.

5.1.9 Alcune applicazioni non funzionano in GNOME con Wayland

GNOME in buster ha cambiato il suo server di visualizzazione predefinito da Xorg a Wayland (vedere Sezione 2.2.11). Alcune applicazioni, incluso il popolare gestore di pacchetti `synaptic`, il metodo di input predefinito per il cinese semplificato, `fcitx`, e la maggior parte delle applicazioni per registrare lo schermo, non sono state aggiornate per funzionare correttamente in Wayland. Per poter usare questi pacchetti è necessario fare il login con una sessione di `GNOME in Xorg`.

5.1.10 Pacchetti obsoleti degni di nota

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

L'elenco dei pacchetti obsoleti comprende:

- Il pacchetto `mcelog` non è più supportato con le versioni del kernel più recenti di 4.12. `rasdaemon` può essere usato come suo rimpiazzo.
- Il pacchetto `revelation`, che è usato per archiviare password, non è incluso in buster. `keepass2` può importare file XML di password precedentemente esportati da `revelation`. Assicurarsi di esportare i propri dati da revelation prima dell'aggiornamento, per evitare di perdere l'accesso alle proprie password.
- Il pacchetto `phpmyadmin` non è incluso in buster.
- `ipsec-tools`e `raconn` sono stati rimossi da buster dato che la fonte originale è in ritardo con gli adattamenti ai nuovi pericoli.

  È consigliato agli utente di migrare a `libreswan`, che ha una più ampia compatibilità del protocollo ed è attivamente mantenuto dagli autori originali a monte.

  `libreswan` dovrebbe essere completamente compatibile in termini di protocolli di comunicazione dato che implementa un sovrainsieme dei protocolli supportati da `racoon`.
- Il semplice MTA `ssmtp` è stato abbandonato per buster. Ciò a causa del fatto che attualmente con convalida i certificati TLS; vedere il bug n.662960 (`https://bugs.debian.org/662960`).
- Il pacchetto `ecryptfs-utils` non fa parte di buster a causa di un grave bug non risolto (nr. 765854 (`https://bugs.debian.org/765854`)). Al momento della stesura di questo paragrafo non esiste un chiaro suggerimento per gli utenti di eCryptfs, a parte non aggiornare.

5.1.11 Componenti deprecati per buster

Con il prossimo rilascio di Debian 11 (nome in codice bullseye) alcune funzionalità diventeranno deprecate. Gli utenti dovranno migrare ad altre alternative per evitare problemi nell'aggiornamento a Debian 11.

Ciò include le seguenti funzionalità:

- Python 2 non verrà più supportato dagli autori a monte a partire dal 1° gennaio 2020 (`https://www.python.org/dev/peps/pep-0373/`). Debian spera di abbandonare `python-2.7` per Debian 11. Se gli utenti hanno funzionalità che si basano su **python** dovrebbero prepararsi a migrare a **python3**.
- Icinga 1.x ha raggiunto la sua fine vita (EOL) per gli autori originali a partire dal 2018-12-31, mentre il pacchetto `icinga` è sempre presente; gli utenti dovrebbero usare la durata di vita di buster per migrare ad Icinga 2 (pacchetto `icinga2`) e Icinga Web 2 (pacchetto `icingaweb2`). Il pacchetto `icinga2-classicui` è ancora presente per usare l'interfaccia web CGI di Icinga 1.x con Icinga 2, ma il supporto per esso verrà rimosso in Icinga 2.11. Si dovrebbe usare invece Icinga Web 2.
- La versione 3 della suite del gestore di mailing-list Mailman è disponibile per la prima volta in questo rilascio. Mailman è stato diviso in vari componenti; la parte principale è disponibile nel pacchetto `mailman3` e la suite completa può essere ottenuta tramite il metapacchetto `mailman3-full`.

  La versione datata 2.1 di Mailman rimane disponibile in questo rilascio nel pacchetto `mailman`, perciò è possibile migrare le installazioni esistenti seguendo i propri ritmi. Il pacchetto di Mailman 2.1 verrà mantenuto in buone condizioni per il prossimo futuro, ma non vedrà grandi modifiche o migliorie. Verrà rimosso dal primo rilascio di Debian successivo all'interruzione del supporto a tale ramo da parte degli autori originali.

  È raccomandato a tutti di aggiornare a Mailman 3, il rilascio moderno in fase di attivo sviluppo.

- I pacchetti `spf-milter-python` e `dkim-milter-python` non sono più mantenuti dagli autori originali a monte, ma sono disponibili in buster i loro rimpiazzi più ricchi di funzionalità: `pyspf-milter` e `dkimpy-milter`. Gli utenti dovrebbero migrare ai nuovi pacchetti prima che i vecchi vengano rimossi in bullseye.

5.1.12 Cose da fare dopo l'aggiornamento prima di riavviare

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

5.1.13 Pacchetti relativi a SysV init non più necessari

NOTA

Questa sezione non si applica a coloro che hanno deciso di rimanere con sysvinit-core.

Dopo il passaggio a systemd come sistema init predefinito avvenuto in Jessie e ulteriormente raffinato in Stretch, vari pacchetti relativi a SysV non sono più necessari e possono essere ora eliminati definitivamente usando

```
apt purge initscripts sysv-rc insserv startpar
```

5.2 Limitazione nel supporto per la sicurezza

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

NOTA

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

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

Debian 10 contiene diversi motori per browser che sono affetti da varie vulnerabilità di sicurezza. L'alto tasso di vulnerabilità e la parziale mancanza di supporto a lungo termine da parte degli autori originali complica l'attività di supporto di questi browser e motori tramite il backport delle correzioni di sicurezza alle versioni precedenti. Inoltre la dipendenza reciproca delle librerie rende estremamente difficile aggiornare a una nuova versione a monte. Perciò, in buster sono presenti browser basati ad esempio sui motori webkit e khtml[1], ma non sono coperti dal supporto di sicurezza. Non si dovrebbe usare questi browser con siti web non fidati. Il pacchetto sorgente `webkit2gtk` è coperto dal supporto di sicurezza.

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

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

5.2.2 Pacchetti basati su Go

L'infrastruttura Debian attualmente non abilita in modo corretto la ricompilazione di pacchetti con link statico a parti di altri pacchetti su larga scala. Fino a buster questo non era in pratica un problema, ma con il crescere dell'ecosistema Go ciò significa che i pacchetti basati su Go non saranno coperti dal regolare supporto di sicurezza fino a che l'infrastruttura non sarà migliorata per poter lavorare con essi in modo mantenibile.

Se sono necessari aggiornmenti, questi possono solamente passare attraverso i regolari rilasi minori, che possono essere lenti ad arrivare.

5.3 Problemi relativi a specifici pacchetti

Nella maggior parte dei casi i pacchetti dovrebbero aggiornarsi senza problemi da stretch a buster. C'è un numero limitato di casi dove può essere necessario un qualche intervento, prima o durante l'aggiornamento; questi casi sono descritti in dettaglio di seguito, pacchetto per pacchetto.

5.3.1 Glibc richiede un kernel Linux 3.2 o successivo

A partire da `glibc` 2.26 è necessario un kernel Linux 3.2 o successivo. Per evitare di rendere il sistema completamente inutilizzabile, lo script di preinstallazione di `libc6` effettua un controllo. Se questo fallisce l'installazione del pacchetto viene abortita, il che lascia l'aggiornamento non terminato. Se il sistema ha in esecuzione un kernel più vecchio di 3.2, aggiornarlo prima di avviare l'aggiornamento della distribuzione.

5.3.2 Semantica cambiata per usare variabili d'ambiente per su

`su` ha cambiato semantica in buster e non preserva più le variabili d'ambiente `DISPLAY` e `XAUTHORITY`. Se si devono eseguire applicazioni grafiche con `su` è necessario impostarle esplicitamente per permettere l'accesso al display. Vedere il bug n.905409 (`https://bugs.debian.org/905409`) per una ampia discussione in merito.

5.3.3 I database PostgreSQL esistenti devono essere reindicizzati

Quando si aggiorna da stretch a buster i dati di localizzazione `glibc` vengono aggiornati. Specificatamente ciò cambia come PostgreSQL ordina i dati negli indici testuali. Per evitare corruzioni, tali indici devono essere reindicizzati con `REINDEX` immediatamente dopo l'aggiornamento dei pacchetti `locales`o `locales-all`, prima di rimettere il database in produzione.

Comando suggerito:

```
sudo -u postgres reindexdb --all
```

In alternativa aggiornare i database a PostgreSQL 11 usando **pg_upgradecluster**. (Questo usa **pg_dump** in modo predefinito il quale recreerà tutti gli indici. L'uso di `-m upgrade` o **pg_upgrade** *non* è sicuro perché preserva l'ordinamento degli indici ora sbagliato.)

Fare riferimento al Wiki di PostgreSQL (`https://wiki.postgresql.org/wiki/Locale_data_changes`) per maggiori informazioni.

5.3.4 mutt e neomutt

In stretch il pacchetto `mutt` aveva patch applicate ai sorgenti da https://neomutt.org (`https://neomutt.org`). A partire da buster, il pacchetto che fornisce `/usr/bin/mutt` è invece basato puramente sui sorgenti originali da http://www.mutt.org (`http://www.mutt.org`) e un pacchetto separato `neomutt` è disponibile e fornisce `/usr/bin/neomutt`.

Ciò significa che alcune delle funzionalità che erano prima fornite da `mutt` ora non sono più disponibili. Se ciò rende difettosa la propria configurazione si può invece installare `neomutt`.

5.3.5 Accesso all'applicazione delle Impostazioni di GNOME senza mouse

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

5.3.6 Il cambio della password LUKS da parte di gnome-disk-utility fallisce causando perdita di dati permanente (solo buster 10.0)

Gli utenti delle immagini del rilascio iniziale di buster non dovrebbero cambiare la password LUKS dei dischi cifrati con l'interfaccia grafica di GNOME per la gestione dei dischi. Il pacchetto `gnome-disk-utility` in buster aveva un serissimo bug (n.928893) (`https://bugs.debian.org/928893`) che si verificava quando usato per modificare la password LUKS: cancellava la vecchia password ma l'impostazione corretta della nuova falliva, rendendo tutti i dati sul disco inaccessibili. Questo problema è stato risolto nel primo rilascio minore.

5.3.7 evolution-ews è stato abbandonato e le caselle di posta che usano server Outlook, Exchange o Office365 verranno rimosse

Gli utenti che usano `evolution` come client di posta e si connettono ad un server con in esecuzione Exchange, Office365 o Outlook usando il plugin `evolution-ews` non dovrebbero aggiornare a buster prima di aver fatto un backup dei dati e aver trovato una soluzione alternativa, dato che evolution-ews è stato abbandonato a causa del bug n.926712 (`https://bugs.debian.org/926712`) e le loro caselle di posta, calendari, elenchi di contatti e attività verranno rimossi e non saranno più accessibili con Evolution.

Il pacchetto `evolution-ews` è stato reintrodotto attraverso buster-backports. Gli utenti che aggiornano da stretch a buster possono abilitare buster-backports dopo l'aggiornamento e saranno quindi in grado di reinstallare `evolution-ews`.

5.3.8 L'installatore di Calamares lascia le chiavi di cifratura del disco leggibili

Quando si installa Debian da supporti live usando l'installatore Calamares (Sezione 2.2.13) e selezionando la funzionalità di cifratura dell'intero disco, la chiave di sblocco del disco viene memorizzata nell'initramfs che è leggibile da tutti. Ciò permette agli utenti con accesso al file system locale di leggere la chiave privata ed ottenere nuovamente accesso al file system in futuro.

Questo problema può essere aggirato aggiungendo `UMASK=0077` a `/etc/initramfs-tools/conf.d/initramfs-permissions` ed eseguendo **update-initramfs -u**. Questo ricrea l'initramfs senza i permessi di lettura per tutti.

Una risoluzione per l'installatore è già in programma (vedere il bug n.931373 (`https://bugs.debian.org/931373`)) e verrà caricata in debian-security. Nel frattempo gli utenti con cifratura dell'intero disco dovrebbero usare la soluzione temporanea descritta sopra.

5.3.9 Cambiamento dell'URL S3QL per i bucket Amazon S3

Quando si usa `s3ql` con bucket Amazon S3 la configurazione deve essere aggiornata per un cambiamento nell'URL. Il nuovo formato è:

```
s3://<regione>/<bucket>/<prefisso>
```

5.3.10 Split in configuration for logrotate

The shipped configurations for `/var/log/btmp` and `/var/log/wtmp` have been split from the main configuration file (`/etc/logrotate.conf`) into separate standalone files (`/etc/logrotate.d/btmp` and `/etc/logrotate.d/wtmp`).

If you have modified `/etc/logrotate.conf` in this regard, make sure to re-adjust the two new files to your needs and drop any references to (b|w)tmp from the main file, since duplicate definitions can cause errors.

5.3.11 The `rescue` boot option is unusable without a root password

With the implementation of `sulogin` now used, booting with the `rescue` option always requires the root password. If one has not been set, this makes the rescue mode effectively unusable. However it is still possible to boot using the kernel parameter `init=/sbin/sulogin --force`

To configure systemd to do the equivalent of this whenever it boots into rescue mode (also known as single mode: see systemd(1) (`https://manpages.debian.org/buster//buster/systemd/systemd.1.html`)), run **sudo systemctl edit rescue.service** and create a file saying just:

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

It might also (or instead) be useful to do this for the `emergency.service` unit, which is started *automatically* in the case of certain errors (see systemd.special(7) (`https://manpages.debian.org/buster//buster/systemd/systemd.special.7.html`)), or if `emergency` is added to the kernel command line (e.g. if the system can't be recovered by using the rescue mode).

For background and a discussion on the security implications see #802211 (`https://bugs.debian.org//802211`).

Capitolo 6

Maggiori informazioni su Debian

6.1 Ulteriori letture

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

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

6.2 Ottenere aiuto

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

6.2.1 Liste di messaggi

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

6.2.2 Internet Relay Chat

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

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

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

6.3 Segnalare i bug

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

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

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

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

6.4 Contribuire a Debian

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

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

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

Capitolo 7

Glossario

ACPI
: Advanced Configuration and Power Interface

ALSA
: Advanced Linux Sound Architecture

BD
: Blu-ray Disc

CD
: Compact Disc

CD-ROM
: Compact Disc Read Only Memory

DHCP
: Dynamic Host Configuration Protocol

DLBD
: Dual Layer Blu-ray Disc

DNS
: Domain Name System

DVD
: Digital Versatile Disc

GIMP
: GNU Image Manipulation Program

GNU
: GNU's Not Unix

GPG
: GNU Privacy Guard

LDAP
: Lightweight Directory Access Protocol

LSB
: Linux Standard Base

LVM
: Logical Volume Manager

MTA
: Mail Transport Agent

NBD
: Network Block Device

NFS
: Network File System

NIC
: Network Interface Card

NIS
: Network Information Service

PHP
: PHP: Hypertext Preprocessor

RAID
: Redundant Array of Independent Disks

SATA
: Serial Advanced Technology Attachment

SSL
: Secure Sockets Layer

TLS
: Transport Layer Security

UEFI
: Unified Extensible Firmware Interface

USB
: Universal Serial Bus

UUID
: Universally Unique Identifier

WPA
: Wi-Fi Protected Access

Appendice A

Gestire il proprio sistema stretch prima dell'avanzamento

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

A.1 Aggiornare il proprio sistema stretch

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

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

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

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

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

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

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 stretch o di buster.

IMPORTANTE

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

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

```
# apt update
```

per aggiornare la lista dei pacchetti.

A.3 Rimuovere file di configurazione obsoleti

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

A.4 Passare dai locale obsoleti a UTF-8

L'uso di una localizzazione non UTF-8 obsoleta da lungo tempo non è più supportato dai desktop e dagli altri progetti software più noti. Tali localizzazioni dovrebbero essere aggiornate usando **dpkg-reconfigure locales** e selezionando un valore predefinito UTF-8. Ci si dovrebbe anche assicurare che gli utenti non scavalchino il valore predefinito per usare una localizzazione obsoleta nel proprio ambiente.

Appendice B

Contributori delle note di rilascio

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

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

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

Indice analitico