Newsletter Ubuntu-it

Numero 025 - Anno 2023

Gruppo Social Media

https://wiki.ubuntu-it.org/GruppoPromozione/

2023

Licenza

Questo documento è stato composto interamente dall'autore con LaTeX. Per maggiori informazioni, o segnalazioni:

Mailing List Newsletter-italiana: iscriviti per ricevere la Newsletter Italiana di Ubuntu!;
Mailing List Newsletter-Ubuntu: la redazione della newsletter italiana. Se vuoi collaborare alla realizzazione della newsletter, questo è lo strumento giusto con cui contattarci.
Canale IRC: *#ubuntu-it-promo*

A cura di:
Daniele De Michele

Newsletter Ubuntu-it

Indice

Questo è il numero **25** del **2023** della Newsletter di Ubuntu-it, riferito alla settimana che va da **lunedì 26 Giugno** a **domenica 2 Luglio**. Per qualsiasi commento, critica o lode, contattaci attraverso la *mailing list* del *gruppo promozione*.

1 Notizie da Ubuntu

1.1 Come accedere all'interfaccia utente LXD

Nel corso degli anni, il team di sviluppo di **Canonical** ha investito molto nella creazione di una CLI LXD intuitiva. Parallelamente, le richieste dagli utenti e dalla community non si sono fatte attendere per ricevere uno strumento *UI* LXD ufficiale, al fine di semplificare il funzionamento delle istanze LXD. Anche la comunità stessa ha cercato di sviluppare in questi anni dei progetti proprio per colmare questa lacuna. Ora però siamo felici di condividere con tutti voi la presenza di un nuovo team, che si concentrerà esclusivamente sull'aumentare e rendere appagante l'esperienza e l'interfaccia utente per chi lavora con LXD. Una di queste funzionalità, denominata "Progetti", aiuta a mantenere pulito un server LXD, raggruppando le istanze correlate. Ogni progetto può avere immagini, profili, reti e storage specifici e gli utenti possono passare facilmente da un progetto all'altro in tutta comodità. È possibile avviare, arrestare, riavviare o bloccare una singola istanza o un gruppo di esse contemporaneamente, nonché accedere al terminale e alla console direttamente dall'interfaccia utente, confezionata insieme allo snap LXD (quindi non sono necessarie installazioni aggiuntive). Tuttavia, dato che si considera ancora la funzione sperimentale, è necessario abilitarla in modo specifico per ottenere l'accesso. Per fare questo, occorre abilitare l'interfaccia utente LXD nello snap, tramite il comando:

```
snap set lxd ui.enable=true
snap restart --reload lxd
```

In secondo luogo, assicuriamoci che il server LXD sia visibile:

```
lxc config set core.https_address :8443
```

Infine, tutto ciò che occorre fare è inserire l'indirizzo del server nel proprio browser (ad esempio, https://192.0.2.10:8443) e seguire le istruzioni che guidano attraverso il processo di autenticazione. Informazioni dettagliate sono disponibili nella *documentazione*, inoltre viene fornito un *video* tutorial, che vi guiderà passo dopo passo per la configurazione del vostro sistema.

Fonte:
ubuntu.com

1.2 Come installare il Kernel Linux 6.4 su Ubuntu 23.04

Buone notizie per tutti gli utenti che usufruisco della distribuzione **Ubuntu**, in quanto ora è possibile installare l'ultima versione del kernel Linux, la **6.4**. Infatti, con il rilascio avvenuto durante la settimana da parte di *Linus Torvalds*, ora gli utenti possono godere di molte fantastiche funzionalità, come un miglior supporto hardware, oltre che svariate correzioni di sicurezza, che permettono di migliorare l'esperienza desktop e renderla più sicura, veloce e affidabile. Ma perché dover aggiornare il proprio kernel, se tutto sommato il proprio sistema funziona correttamente? La risposta a tale domanda è molto semplice, in quanto si aggiorna il kernel della propria distribuzione se si ha bisogno di una o più funzionalità (introdotte con la nuova versione) che permettono di utilizzare un componente hardware nel migliore dei modi. Per questo, oggi, con questo articolo vedremo come installare la versione 6.4 del kernel su **Ubuntu 23.04**, dato che le altre distribuzioni, come Arch Linux, openSUSE Tumbleweed o Fedora Linux ricevono immediatamente il kernel attraverso i loro repository software. Con Ubuntu, invece, occorre procedere manualmente. Per fare ciò, utilizzeremo la *CLI* (Command-line interface), insieme ai *pacchetti del kernel* dall'archivio PPA di Ubuntu, forniti direttamente da Canonical. Con l'unica precisazione che i suddetti pacchetti del kernel, pur essendo creati dall'Ubuntu Kernel Team, non sono firmati, il che significa che non possono essere installati su sistemi che hanno il Secure Boot abilitato. Pertanto, prima di procedere, occorre disabilitare Secure Boot. L'installazione tramite CLI è abbastanza semplice, infatti basterà scaricare, per la propria architettura, i pacchetti del kernel Linux 6.4 e salvarli in una cartella sotto Home. Successivamente, aprire il Terminale e spostarsi nella cartella dove sono salvati i file (ad esempio cd ∼/Scaricati) ed eseguire il comando:

```
sudo dpkg -i *.deb
```

e attendere fino al completamento del processo di installazione, quindi riavviare il computer. Qualora si volesse eseguire l'aggiornamento a future versioni, si dovrà scaricare manualmente i nuovi pacchetti dall'archivio PPA del kernel di Ubuntu e ripetere questa procedura. Se invece si preferisce evitare la linea di comando, si può sempre usare l'utility *Ubuntu Mainline Kernel Installer*. Il gioco è fatto ;)

Fonte:
9to5linux.com

1.3 Canonical si unisce all'Eclipse Foundation

Canonical, la società dietro la famosa distribuzione **Ubuntu**, è entusiasta di annunciare la sua adesione all'*Eclipse Adoptium Working Group*. Per chi non lo sapesse, l'*Eclipse Adoptium Working Group* è una piattaforma collaborativa a cui partecipano aziende del calibro di Alibaba, Azul, Huawei, IBM, Microsoft, Red Hat, Rivos e, più recentemente, Google, che promuove l'innovazione, lo sviluppo e la distribuzione di toolchain Java basate sul progetto *OpenJDK*. Dal canto suo, Canonical, attraverso questa stretta collaborazione, continuerà a far progredire, promuovere e diffondere toolchain di alta qualità e tecnologie correlate in tutta la comunità Java e anche all'interno del suo sistema operativo

Ubuntu. Staremo a vedere :)

Fonte:
ubuntu.com

1.4 In arrivo un nuovo look per il sito snapcraft.io

Dopo aver mantenuto la stessa interfaccia utente e lo stesso stile per diversi anni, il team di sviluppo di **Canonical** ha intrapreso un nuovo progetto per ridisegnare completamente l'intero sito *snapcraft.io* e dargli un aspetto molto più moderno. Prima di poter procedere, è stato necessario analizzare e pianificare come migliorare lo store, suddividendo i compiti da svolgere in due fasi: la prima fase è stata un *rebranding* per aggiornare l'aspetto del sito, che implica un allineamento del marchio, insieme ai colori principali, tra i vari siti Canonical, per offrire un'esperienza più coerente tra i prodotti. La seconda fase è ora in corso, perché non si vuole semplicemente aggiornare l'aspetto di snapcraft.io, ma anche ottimizzare le pagine stesse. Per questo motivo,l si sta analizzando nel complesso la facilità d'uso del sito e anche le varie aree di miglioramento per valutare come ristrutturare le informazioni attualmente visualizzate negli elenchi di snap, per renderle il più utili possibile agli occhi degli utenti. Inoltre, si sta studiando anche come strutturare i vari tutorial e le rispettive documentazioni per rendere il processo di creazione dei pacchetti snap il più snello e facile possibile. Infine, l'elenco degli snap, che risulterà essere in primo piano, verrà aggiornato più frequentemente con diversi snap, questo servirà a dare maggiore visibilità a una gamma di editori/sviluppatori. Per comprendere se le azioni che si stanno eseguendo siano coerenti, compila il *sondaggio* e facci conoscere i tuoi pensieri.

Fonte:
ubuntu.com
omgubuntu.co.uk

1.5 Canonical rilascia nuovi aggiornamenti di sicurezza per il Kernel Linux

Canonical ha rilasciato nuovi aggiornamenti di sicurezza del kernel Linux per tutte le versioni di Ubuntu supportate, per affrontare tre vulnerabilità di sicurezza scoperte e segnalate da vari ricercatori di sicurezza. Per tutte le suddette versioni di Ubuntu, troviamo che il nuovo aggiornamento di sicurezza corregge una vulnerabilità (*CVE-2023-35788*) scoperta da Hangyu Hua nell'implementazione del Flower classifier del kernel e un difetto che interessa i processori Intel causato dall'impossibilità dell'implementazione dell'istruzione INVLPG di eliminare correttamente le voci TLB globali quando i PCID sono abilitati. Entrambi i difetti potrebbero consentire a un utente malintenzionato di causare un crash del sistema o eseguire codice arbitrario portando a esporre informazioni sensibili. Invece, per i soli sistemi **Ubuntu 22.10** e **22.04 LTS** che eseguono il kernel Linux 5.19, si risolvono in ordine: una vulnerabilità di sicurezza (*CVE-2023-2430*), scoperta da Xingyuan Mo e Gengjia Chen nel sottosistema *io_uring* del kernel Linux, che potrebbe consentire a un utente malintenzionato locale di causare un arresto anomalo del sistema. Come sempre, **Canonical**

esorta tutti gli utenti di **Ubuntu** ad aggiornare quanto prima le proprie installazioni alle nuove versioni del kernel. Ricordiamo che per fare ciò, basterà eseguire il comando da terminale:

```
sudo apt update && sudo apt full-upgrade
```

oppure ancora si può utilizzare Ubuntu Software Center. Non dimenticare di riavviare il sistema dopo aver installato la nuova versione del kernel.

Fonte:
9to5linux.com

1.6 Rafforzare la propria sicurezza informatica con Ubuntu Pro

Nel panorama digitale odierno, le organizzazioni di tutte le dimensioni hanno ampliato e proiettato la propria presenza all'interno dei sistemi cloud. Parallelamente a questa espansione, però, arriva un aumento significativo della superficie di attacco, rendendo l'argomento sicurezza una delle principali preoccupazioni delle varie aziende. In questo articolo cercheremo di immergerci nell'entusiasmante mondo della sicurezza informatica all'interno dei cloud ed esploreremo un approccio per proteggere i carichi di lavoro con l'aiuto di **Ubuntu**.
Questa distribuzione offre molte funzionalità di sicurezza integrate, come una completa crittografia del disco, il controllo dell'accesso obbligatorio tramite *AppArmor*, varie funzionalità del file system e l'avvio sicuro tramite *UEFI*. Per migliorare ulteriormente la propria posizione di sicurezza, è possibile abilitare funzionalità di sicurezza aggiuntive con un abbonamento *Ubuntu Pro* (ricordando che Ubuntu Pro è gratuito per un massimo di cinque macchine per uso commerciale personale e su piccola scala o fino a cinquanta macchine per i membri ufficiali della comunità Ubuntu), in cui troviamo:

1. **Ampia copertura di sicurezza**: Ubuntu Pro fornisce patch di sicurezza complete per oltre 25mila pacchetti open source, incluse applicazioni popolari come Apache Kafka, NGINX, MongoDB, Redis e PostgreSQL;

2. **Tempi di inattività ridotti**: con il *servizio Livepatch* di Ubuntu Pro, è possibile usufruire di patch istantanee per CVE elevati e critici del proprio kernel in fase di esecuzione, senza la necessità di un riavvio immediato. Ciò può ridurre notevolmente le interruzioni dell'attività e massimizzare il tempo di attività nel proprio server;

3. **Dieci anni di stabilità della piattaforma**: Canonical garantisce dieci anni di manutenzione della sicurezza per gli utenti di Ubuntu Pro che eseguono versioni LTS, garantendo un decennio di stabilità e protezione per i propri carichi di lavoro;

4. **Certificazioni di conformità**: Ubuntu Pro offre strumenti di automazione e controllo per *DISA-STIG*, *rafforzamento e controllo CIS*, moduli crittografici certificati *FIPS* e altro ancora.

5. **Supporto 24/7**: con Ubuntu Pro è disponibile anche il *supporto opzionale* nei giorni feriali o 24/7, assicurandoti l'assistenza di esperti ogni volta che

ne hai bisogno. Include la risoluzione dei problemi, la correzione di guasti e bug su 25 mila pacchetti open source e un'ampia gamma di applicazioni, con un tempo di prima risposta di un'ora per problemi critici.

Sebbene il rafforzamento della sicurezza e l'applicazione automatica di patch CVE siano essenziali per proteggere i carichi di lavoro del cloud da vulnerabilità di sicurezza note, non è possibile proteggere i dati dalle vulnerabilità zero-day all'interno del software di sistema nel cloud o da un provider di servizi cloud potenzialmente dannoso. Questo perché, fino a poco tempo fa, non erano disponibili meccanismi per proteggere i carichi di lavoro sensibili in fase di esecuzione. Oggigiorno invece vengono in soccorso modalità di esecuzione isolate delle applicazioni, come gli snap. Per saperne di più su questo argomento, ti invitiamo a leggere un *white paper* che fornisce una discussione approfondita sull'adozione di un approccio più forte alla sicurezza informatica del cloud di Azure con **Ubuntu**.

Fonte:
ubuntu.com

2 Notizie dalla comunità internazionale

2.1 Full Circle Magazine Issue #194 in inglese

È stato pubblicato sul sito internazionale di *Full Circle Magazine*, il numero 194 in Inglese. In questo numero troviamo:

- Comanda & Conquista
- How-To: Python, Stable Diffusion e Latex
- Grafica: Inkscape
- Grafica: FreeCAD
- Micro This Micro That
- Recensione: Kubuntu 23.04
- Recensione del libro: guida completa alla grafica di Blender
- Giochi Ubuntu : APICO

... e molto altro ancora. È possibile scaricare la rivista da *questa pagina*.

3 Notizie dal Mondo

3.1 Libreboot: un'alternativa al classico Bios

Se non lo conoscete ancora, *Libreboot* è un progetto open source, nato nel lontano 2013, che mira a fornire un'alternativa libera e open source al BIOS e che si allinea alle linee guida emanate dalla **Free Software Foundation**. Dopo quasi un anno di duro lavoro, di recente è stata annunciata una nuova versione

di **Libreboot**, che introduce il supporto per il nuovo hardware, oltre a numerosi miglioramenti, consentendo a più persone di utilizzare questa soluzione open source sui loro computer. Primo tra tutti, si implementa il supporto per le nuove schede madri sia per laptop sia per computer desktop, tra cui HP EliteBook 2570p, HP 8300 USDT e Gigabyte GA-G41M-ES2L. Al momento della stesura di questo articolo, Libreboot funziona bene anche su dispositivi Acer G43T-AM3, Apple iMac 5,2, Intel D510MO e D410PT, nonché su Apple MacBook1,1 e MacBook2,1, Dell Latitude E6400, HP EliteBook 2560p e HP EliteBook Folio 9470m. La nuova versione include anche una ROM senza *microcodice* per la CPU e starà all'utente scaricare l'immagine ROM che contiene microcodice CPU o meno. Oltre a ciò, Libreboot ha ricevuto un enorme elenco di modifiche al sistema di compilazione, con metà del codice riscritto o sottoposto a pesante refactoring, nel tentativo di migliorare ulteriormente lo stile di codifica e correggere più bug. Per maggiori informazioni riguardanti le modifiche apportate a questa build, dai un'occhiata alla *pagina* dell'annuncio di rilascio.

Fonte:
omglinux.com
9to5linux.com

4 Aggiornamenti e statistiche

4.1 Aggiornamenti di sicurezza

Gli annunci di sicurezza sono consultabili nell'apposita *sezione del forum*.

4.2 Bug riportati

- Aperti: 142217, +**45** rispetto alla scorsa settimana.
- Critici: 317, +**3** rispetto alla scorsa settimana.
- Nuovi: 71369, **-36** rispetto alla scorsa settimana.

È possibile aiutare a migliorare Ubuntu, riportando problemi o malfunzionamenti. Se si desidera collaborare ulteriormente, la *Bug Squad* ha sempre bisogno di una mano.

4.3 Statistiche del gruppo sviluppo

Segue la lista dei pacchetti realizzati dal *GruppoSviluppo* della comunità italiana nell'ultima settimana:

- *Mattia Rizzolo*:
  - *libexecs 1.4-2*, per Debian unstable

Se si vuole contribuire allo sviluppo di Ubuntu correggendo bug, aggiornando i pacchetti nei repository, ecc... il *GruppoSviluppo* è sempre alla ricerca di nuovi volontari.

5 Commenti e informazioni

La tua newsletter preferita è scritta grazie al contributo libero e volontario della *comunità ubuntu-it*. In questo numero hanno partecipato alla redazione degli articoli:

- *Daniele De Michele*

Ha inoltre collaborato all'edizione:

- *Stefano Dall'Agata*
- *Massimiliano Arione*

Ha realizzato il pdf:

- *Daniele De Michele*

6 Scrivi per la newsletter

La **Newsletter Ubuntu-it** ha lo scopo di tenere aggiornati tutti gli utenti **Ubuntu** e, più in generale, le persone appassionate del mondo open-source. Viene resa disponibile gratuitamente con cadenza settimanale ogni Lunedì, ed è aperta al contributo di tutti gli utenti che vogliono partecipare con un proprio articolo. L'autore dell'articolo troverà tutte le raccomandazioni e istruzioni dettagliate all'interno della pagina *Linee Guida*, dove inoltre sono messi a disposizione per tutti gli utenti una serie di indirizzi web che offrono notizie riguardanti le principali novità su Ubuntu e sulla comunità internazionale, tutte le informazioni sulle attività della comunità italiana, le notizie sul software libero dall'Italia e dal mondo. Per chiunque fosse interessato a collaborare con la newsletter Ubuntu-it a titolo di redattore o grafico, può scrivere alla *mailing list* del *gruppo promozione* oppure sul canale IRC: *#ubuntu-it-promo*. Fornire il tuo contributo a questa iniziativa come membro, e non solo come semplice utente, è un presupposto fondamentale per aiutare la diffusione di Ubuntu anche nel nostro paese. Per rimanere in contatto con noi, puoi seguirci su:

Facebook *Twitter* *YouTube* *Telegram*

"Noi siamo ciò che siamo per
merito di ciò che siamo tutti"

Questa newsletter è stata prodotta dal
Gruppo Social Media usando esclusivamente
software libero.