Naps2: Kompaktes Steuerzentrum für Scanner S. 46

09.2025

linuxUSER

linuxUSER

AXOS • DEBIAN „TRIXIE" • LEGO SPIKE • LGM 2025 • NAPS2 • PIPEWIRE • DOCKER IM GRIFF

09

Containervirtualisierung auf dem Desktop mit Docker und Docker Compose

DOCKER IM GRIFF

Werkzeugkasten: Docker und Docker Compose optimal konfigurieren S. 20

Alltagsbetrieb: Dienste und Apps in Containern einrichten und verwalten S. 28

Grafische Docker-Frontends: Mehr Bedienkomfort mit Portainer, Docker Desktop und Yacht S. 36

AxOS: Handliches Arch-Linux-Derivat mit Pfiff S. 6

Gertenschlanker Arch-Linux-Ableger mit komfortablen grafischen Verwaltungswerkzeugen und innovativen Desktop-Oberflächen

Debian 13 „Trixie" S. 74

Stabilität im Fokus: Ausblick auf das kommende Debian-Release

Lego Education Spike S. 66

Robotik-Baukasten bringt Kids die Informatik spielerisch nahe

Höhere Sicherheit für OpenSuse S. 58
Leap-Installationen mit simplen Mitteln besser gegen Schadsoftware schützen

Mehr Durchblick im Lizenzwirrwar S. 88
Alle wichtigen Lizenzen für Open Source und freie Software im Detail erklärt

www.linux-user.de

EUR 8,99 Deutschland | EUR 9,70 Österreich | sfr 14,00 Schweiz | EUR 10,40 Benelux

4 195111 008994 09

Schwerter zu Quellcode

Jörg Luther
Chefredakteur

Liebe Leserinnen und Leser,

seit dem Amtsantritt von US-Präsident Donald Trump machen die Abhängigkeit der Europäer von den USA und deren Folgen immer wieder Schlagzeilen. Die ist vor allem im Verteidigungsbereich so hoch, dass sich die NATO-Staaten zu einer geradezu abstrusen Erhöhung der Militärbudgets auf 5 Prozent des Bruttoinlandsprodukts (BIP) gezwungen sehen. Dabei gibt das nordatlantische Noch-Bündnis schon heute mehr Geld für Rüstung aus als der gesamte Rest des Planeten, und selbst die Ukraine – ein Land im Krieg! – kommt mit 2,9 Prozent des BIP für Rüstung aus. Aber es hilft nichts: Um nicht zu riskieren, die für ihre Verteidigung unabdingbaren, nicht ersetzbaren Aufklärungs- und Kommunikationsmittel des US-Militärs einzubüßen, schlucken die Europäer selbst unsinnige US-Zölle fast ohne erkennbaren Widerstand. Ihnen bleibt keine andere Wahl.

Die hätten sie aber an anderer Stelle: bei der digitalen Souveränität. Dass Europa sich auch in Sachen Hard- und Software von den USA abhängig gemacht hat, produziert zwar anders als Rüstung und Zölle keine Schlagzeilen, ist jedoch keineswegs weniger dramatisch.

Weitere Infos und interessante Links
www.linux-user.de/qr/52025

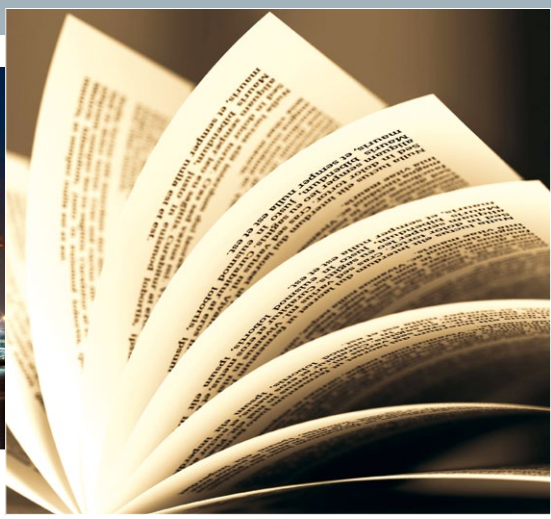
Ob Staat oder Wirtschaft: Die Europäer setzen auf Rechner von US-amerikanischen Hardwarefirmen und fahren darauf Programme von US-Softwareanbietern, wenn sie denn ihre Daten nicht gleich in die Clouds von nordamerikanischen Konzernen befördern. Zumindest in Sachen Software tut das nun wirklich nicht not, denn schließlich gibt es eine probate Alternative: Open Source. Freie Software bietet das Potenzial, sich in Sachen Software und Dienste komplett aus der Abhängigkeit von anderen Staaten und Großkonzernen zu befreien.

Schon heute bilden Open-Source-Komponenten die Grundlage zahlreicher Produkte, darunter auch vieler kommerzieller Lösungen. Allerdings erhalten viele Open-Source-Projekte keine Einnahmen und stoßen so immer wieder an ihre Grenzen. Dabei steuern sie mindestens 65 Milliarden Euro zur europäischen Wirtschaft bei. Dennoch kann nur ein Drittel aller Maintainer von ihrer Arbeit leben. Zumindest Deutschland hat das schon erkannt und arbeitet über Einrichtungen wie das Zentrum für Digitale Souveränität (ZenDiS) und die Sovereign Tech Agency an der Förderung von Open-Source-Projekten und -Technologien. Auf europäischer Ebene dagegen gibt es bislang nichts Vergleichbares. Jetzt kommt von Github ein Vorschlag, der darauf abzielt, das zu ändern.

Dazu fordert die Softwareentwicklungsplattform einen neu zu schaffenden europäischen Fördertopf. Hierfür hat Github eigens eine Studie in Auftrag gegeben, die beschreibt, wie man den bereits erfolgreichen deutschen Sovereign Tech Fund auf die gesamte EU übertragen könnte. Der neue Fonds soll kritische Open-Source-Abhängigkeiten innerhalb der EU identifizieren, in die Wartung und Sicherheit von freien Softwarekomponenten investieren, Verbesserungen finanzieren und das Open-Source-Ökosystem insgesamt stärken. Als Rahmenbedingungen fordert Github eine minimale Bürokratie, politische Unabhängigkeit, Flexibilität bei der Vergabe und Transparenz.

Die Kosten für eine solche Initiative wären überschaubar: 350 Millionen Euro veranschlagen die Autoren der Studie, das Open Forum Europe, das Fraunhofer ISI und das European University Institute dafür. Das wäre bei angedachten 100 Milliarden Euro für Panzer, Flugabwehr und Infrastruktur geradezu aus der Portokasse zu finanzieren, brächte Europa aber ein großes Stück weiter auf dem Weg heraus aus der US-Abhängigkeit und hin zur digitalen Souveränität.

Herzliche Grüße,



20 **Docker und Docker Compose** lassen sich auf den gängigen Distributionen wie Debian oder Fedora im Handumdrehen installieren.

28 Via Docker Compose können Sie **Apps und Dienste in Docker** sowohl im Terminal als auch per GUI einrichten. Wir stellen einige Programme vor, die den Umgang und das Orchestrieren mehrerer Container vereinfachen.

46 Bilder und Texte einscannen, durchsuchbare PDFs erstellen und den Scanner im LAN teilen: Das funktioniert mit **Naps2** problemlos.

Heft-DVD

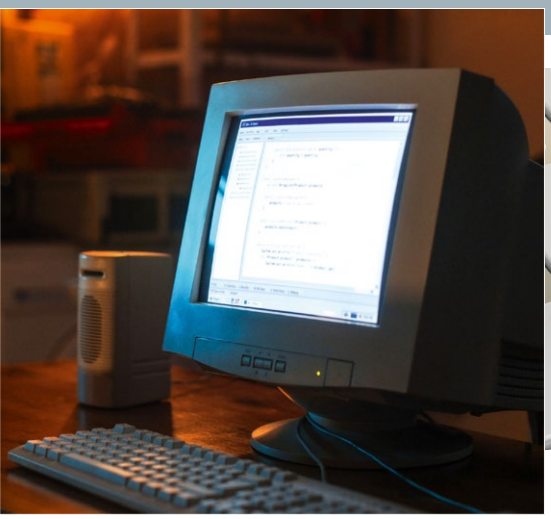
Report

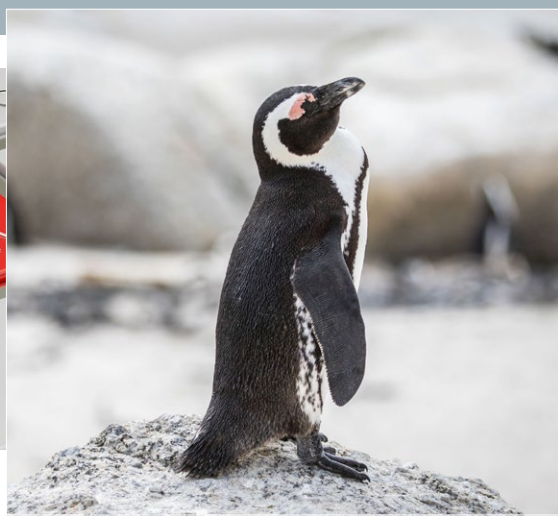
Aktuelles

Schwerpunkt

Schwerpunkt

6 Das auf Arch Linux basierende AxOS möchte durch Einführung grafischer Werkzeuge die unbequeme Systemverwaltung von Arch erleichtern. Außerdem sollen neue, sehr schlanke Arbeitsoberflächen das gesamte System wesentlich agiler wirken lassen.





50 Der Protagonist Evan Tanner kämpft im Spiel **The Operator** noch mit seinem Kater, als er seinen neuen Job als Operator beim FDI antritt.

58 Die **OpenSuse-Tipps** beschäftigen sich mit der Frage, wie sich die Sicherheit des Systems gegenüber dem Auslieferungszustand noch verbessern lässt. Trotz guter Vorarbeit der Maintainer bleibt da Luft nach oben.

74 Das kommende Major Release **Debian 13 „Trixie“** offeriert frischere Pakete, bleibt aber der Debian-Linie treu: stabil und zuverlässig.

Praxis

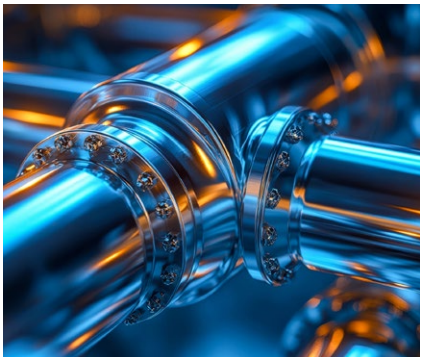
easyLINUX!

.

80 Der moderne Audio/Video-Server **Pipewire** räumt bei voller Kompatibilität gründlich mit den Unzulänglichkeiten seines Vorgängers Pulseaudio auf und bietet einen optimalen Kompromiss aus automatischer Konfiguration und maximaler Flexibilität.

Raspberry Pi

Netz&System



Netz&System

Know-how

Service

Arch-Linux-Derivat AxOS unter der Lupe

Schlankheitskur

Die gängigen grafischen Arbeitsumgebungen wie Gnome oder KDE Plasma werden immer größer und träger. AxOS zeigt, dass nutzerfreundliche Arbeitsoberflächen auch schlank ausfallen können. Erik Bärwaldt

README

Das auf Arch Linux basierende AxOS will durch Einführung grafischer Werkzeuge die unbequeme Systemverwaltung von Arch erleichtern. Außerdem sollen neue, sehr schlanke Arbeitsoberflächen das gesamte System wesentlich agiler wirken lassen. Ob das gelingt, zeigt unser Test mit verschiedenen Arbeitsumgebungen.

Die konventionellen grafischen Desktop-Umgebungen wie Gnome oder KDE Plasma entwickeln einen immer höheren Ressourcenbedarf. So zwingen sie ältere Hardware mit kleinerem Arbeitsspeicher schnell in die Knie, wenn Sie zusätzlich optische Effekte aktivieren.

Am anderen Ende des Spektrums buhlen besonders ressourcenschonende Window-Manager wie IceWM oder Fluxbox um die Gunst der Anwender. Sie haben jedoch in aller Regel einen gravierenden Nachteil: Die Bedienung ist ungewöhnlich und schreckt damit Um- und Einsteiger ab. Außerdem müssen viele Einstellungen wegen fehlender grafischer Konfigurationswerkzeuge manuell an Textdateien vorgenommen werden, was wegen der Komplexität der Syntax selbst so manchem alten Hasen Bauchschmerzen bereitet.

Einen anderen Ansatz verfolgt das aus Frankreich stammende AxOS. Die auf Arch Linux basierende Distribution modifiziert schlanke Window-Manager und ermöglicht so auch auf älterer Hardware ein angenehmes Benutzererlebnis, ohne dass der Desktop den Charme antik-verstaubter Muffigkeit versprüht.

AxOS legt den Schwerpunkt nicht auf möglichst viele Innovationen „unter der Haube". Es bringt außer einer neuen Paketverwaltung namens Epsilon und Axcontrol, einem Werkzeug zum Monitoring des Systems, keine eigenen neuen Programme mit. Die beiden Tools erfor-

dern eine Bedienung auf der Kommandozeile. Dafür bietet das Arch-Derivat eine Auswahl von vier unterschiedlichen Arbeitsumgebungen, von denen nur KDE Plasma zu den gängigen Arbeitsoberflächen zählt. Bei den anderen drei handelt es sich um brandneue Entwicklungen, die aber teilweise auf etablierten Window-Managern basieren. Dabei kommen auch wenig bekannte Komponenten zum Einsatz, darunter der noch junge Wayland-Fork Hyprland Compositor. Die kleineren Desktop-Varianten basieren zudem auf Tiling-Window-Managern und lassen sich somit auch bequem mit der Tastatur bedienen.

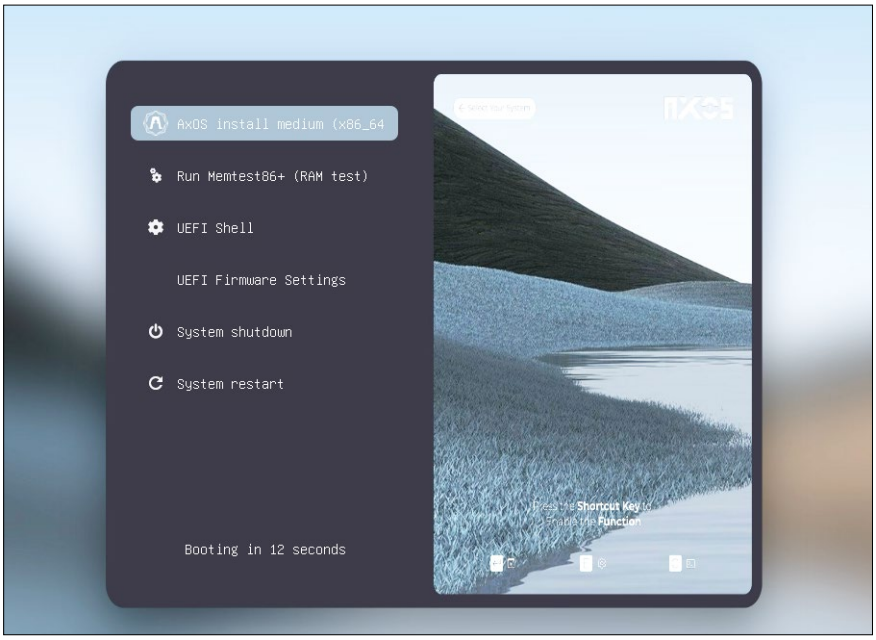
Das Arch-Derivat gibt sich außerordentlich genügsam. So benötigt es im Leerlauf lediglich etwa 850 MByte RAM, womit es sich auch für ältere Rechner mit 2 GByte Hauptspeicher eignet. Für das flüssige Arbeiten mit großen Programmen wie Gimp sollten aber besser 4 GByte RAM im Rechner stecken.

Paketverwaltung

AxOS bringt eine eigene, zu Pacman kompatible Paketverwaltung namens Epsilon mit. Sie bedienen sie komplett auf der Kommandozeile mithilfe einer auch für Einsteiger leicht verständlichen Syntax. Sie integriert außer Arch-Linux-Repositories ein AxOS-eigenes Softwarearchiv. Dadurch installieren Sie zusätzliche Anwendungen am Prompt. Unter dem Sleex-Desktop steht außerdem mit dem Programm Packages ein grafisches Frontend bereit, das diesen Job übernimmt. Darüber hinaus erlaubt AxOS das Verwenden von Pacman, der Paketverwaltung von Arch Linux.

Erste Schritte

AxOS gibt es in Form zweier ISO-Abbilder für 64-Bit-PCs. Anwender mit Intel- oder AMD-Grafikkarte wählen das Abbild *AxOS 25.06* (1,9 GByte). Nutzer von Nvidia-Grafikadaptern laden stattdessen *AxOS 25.06 NVIDIA* (2,5 GByte). Beachten Sie, dass AxOS ausschließlich auf Systemen mit aktiviertem UEFI statt eines herkömmlichen BIOS startet. Auch ältere Computer, die UEFI in Verbindung mit einem Legacy-Modus nutzen, eignen sich nicht zum Betrieb von AxOS.

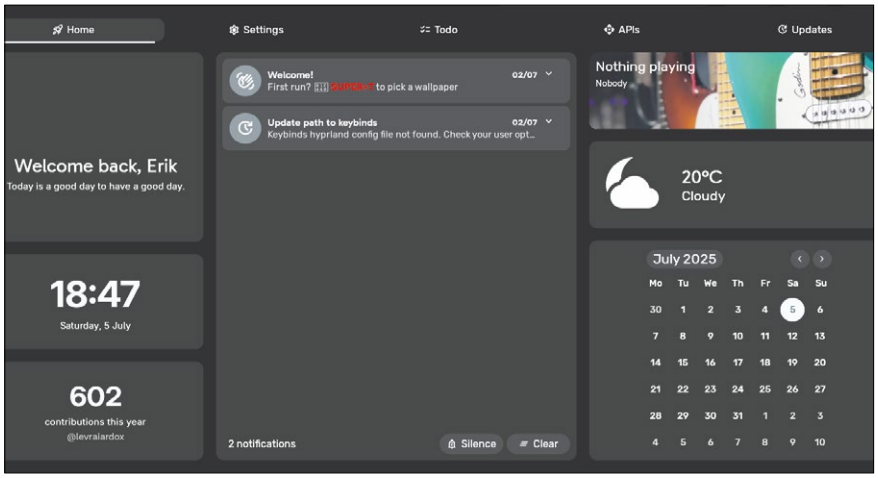


1 Der Bootmanager von AxOS gibt sich optisch sehr ansprechend.

Nach dem Transfer des heruntergeladenen Abbilds auf einen Wechseldatenträger, zum Beispiel einen USB-Stick, starten Sie Ihren Computer davon. Schon der Bootmanager präsentiert sich optisch sehr ansprechend mit einer Installationsoption 1. Nach deren Aufruf bootet das System in den Live-Modus und aktiviert die vom Projekt selbst entwickelte grafische Installationsroutine Axinstall.

Sie weist im Falle einer fehlenden Internetverbindung zunächst darauf hin, diese herzustellen. Das Problem tritt nur bei einem WLAN-Zugang auf, kabel-

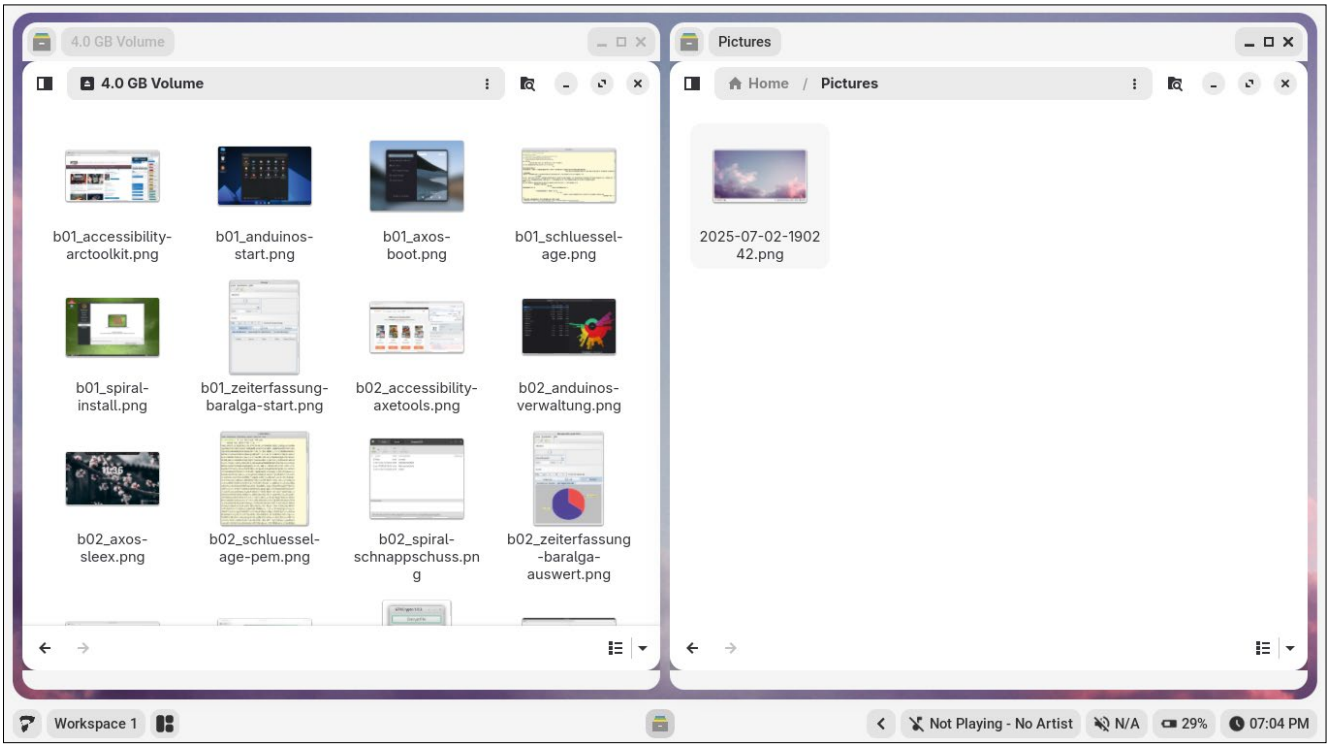
2 Der Sleex-Desktop bedarf nur geringer Einarbeitung.



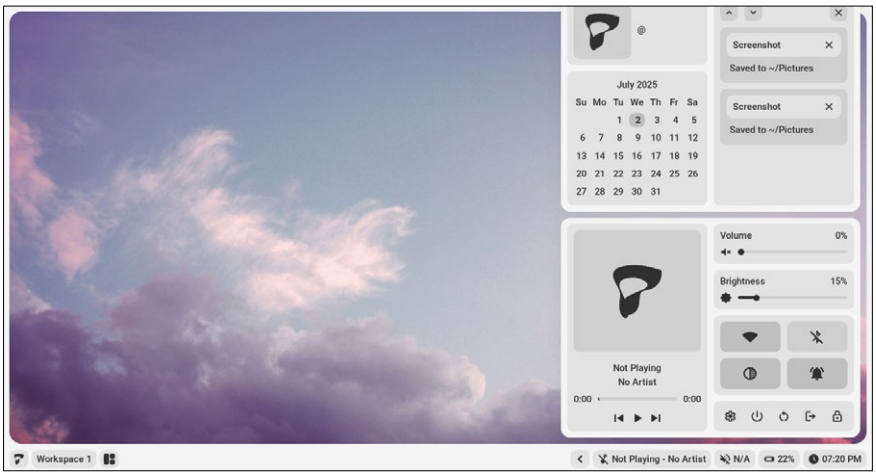
3 Mithilfe eines eigens entwickelten Dashboards nehmen Sie einige Einstellungen bequem grafisch vor und verwalten auch Ihre Termine.

gebundene Anschlüsse aktiviert das System beim Hochfahren automatisch. Um einen WLAN-Zugang einzuschalten, klicken Sie oben rechts im System-Tray auf das durchgestrichene WLAN-Symbol und im Konfigurationswerkzeug oben links auf den Eintrag *Settings*. Danach suchen Sie das gewünschte WLAN aus und geben den dazugehörigen WPA-Schlüssel ein. Ein Druck auf die Eingabetaste stellt die Verbindung unverzüglich her.

Danach klicken Sie in der Installationsroutine auf *Start*. Im ersten Dialog legen Sie die Tastaturbelegung, die Lokalisierung sowie die Zeitzone, das Datum und die Zahlennotation fest. Im nächsten Schritt legen Sie einen Benutzer an, den Sie bei Bedarf mit Administratorrechten



4 Der gewöhnungsbedürftige Calla-Desktop befindet sich derzeit noch in einem sehr experimentellen, praktisch kaum nutzbaren Zustand. Aus diesem Grund eignet er sich bestenfalls dafür, ihn in der Live-Version näher zu begutachten.



5 Der Calla-Desktop blendet auf Wunsch auch Statusinformationen ein. Darüber hinaus regeln Sie damit elementare Einstellungen wie Helligkeit und Lautstärke.

ausstatten. Im folgenden Dialog bestimmen Sie die Arbeitsumgebung. Zur Auswahl stehen KDE Plasma, Calla und Sleex. Voreingestellt kommt in der Live-Version letztere zum Zug. Den Calla-Desktop gibt es bislang nur für Debian.

Nach einem Klick auf *Next* wählen Sie im folgenden Fenster einen Kernel aus. Neben dem Standard-Kernel steht ein leistungsoptimierter Linux-Zen-Kernel zur Wahl. Im folgenden Dialog wählen Sie zwischen den verschiedenen Anwendungssammlungen. Die jeweiligen Paketarchive aktivieren Sie mit dem Schieberegler rechts vom Eintrag. In dieser Auswahl installieren Sie bei Bedarf die Nvidia-Treiberpakete.

Im vorletzten Dialog stellen Sie das Installationsziel ein. Entsprechende Schaltflächen erlauben dabei ein manuelles Partitionieren. Abschließend erscheinen nochmals alle getätigten Einstellungen in einem Fenster. Ein Klick auf das Stiftsymbol neben den Einträgen erlaubt das nachträgliche Ändern.

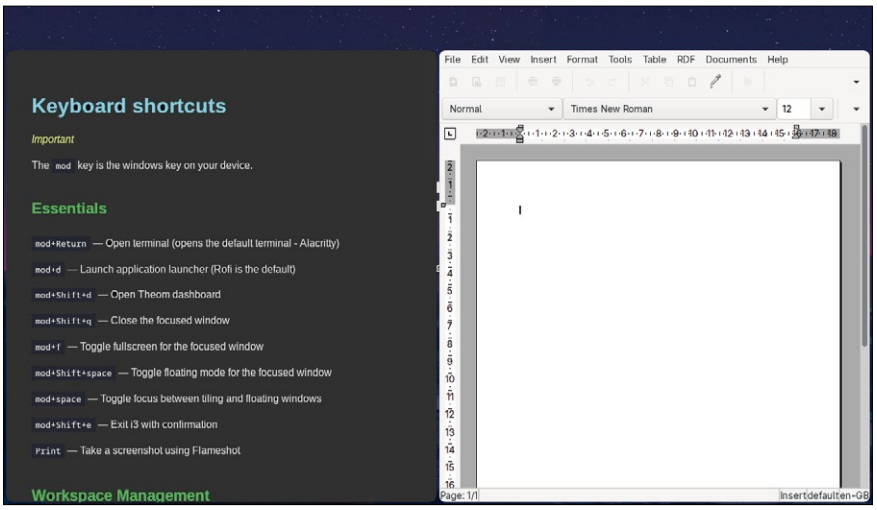
Nach dem abschließenden Klick auf *Next* startet die Installation, und ein eingeblendetes Terminalfenster visualisiert deren Fortschritt. Beachten Sie, dass dieser Prozess längere Zeit in Anspruch nimmt, weil die Distribution zahlreiche Pakete aus dem Internet nachlädt.

Erster Start

Nach Abschluss der Installation starten Sie Ihren Rechner neu. Sie gelangen in einen ansprechenden Login-Dialog und danach zum Desktop. Dieser fällt durch seine ungewöhnliche Gestaltung auf, die jedoch dank der logischen Anordnung der Bedienelemente auf Anhieb vertraut wirkt. Sollten Sie kein kabelgebundenes Netzwerk betreiben, gilt es, den WLAN-Zugang erneut einzurichten.

Der als primäre Arbeitsoberfläche für das Arch-Linux-Derivat konzipierte Sleex-Desktop arbeitet mit dem Hyprland-Compositor. Der Tiling-Window-Manager lässt sich komplett mit der Tastatur bedienen. Mithilfe bestimmter, zum Teil konfigurierbarer Shortcuts können Sie schnell innerhalb der Arbeitsoberfläche navigieren und Funktionen aufrufen.

Sleex kommt mit einer dreigeteilten Panel-Leiste am oberen Bildschirmrand. Links befindet sich eine Angabe zur verwendeten virtuellen Arbeitsoberfläche,



6 Auch die Theom-Oberfläche stellt die Fenster neben- und übereinander dar.

die auch als Startmenü dient. Mittig finden Sie acht Arbeitsoberflächen, die sich hinter einer Leiste von Punkten verbergen. Links und rechts daneben gibt es einige Statusanzeigen, etwa zur Auslastung des Hauptspeichers oder der Temperatur der CPU. Rechts zeigt die Leiste die aktuelle Zeit und das Datum an.

Ganz rechts am Bildschirmrand befindet sich ein System-Tray, der unter anderem den Ladezustand eines Laptop-Akkus anzeigt. Ebenfalls mit im Boot sind eine WLAN-, Lautstärke- und Bluetooth-Anzeige. Rechts unten auf dem Desktop geben zwei grafische Statusanzeigen Auskunft über die Belegung von Arbeits- und Massenspeicher 2.

Ein Klick auf das Startmenü oben links listet einige installierte Programme auf und präsentiert darüber eine Suchleiste. Je nach Eingabe ändert sich die Liste der darunter angezeigten Anwendungen. Meist genügt die Eingabe von drei bis vier Buchstaben, um die gewünschte Software zu finden. Zusätzlich installierte Software erscheint jedoch erst dann im Menü, wenn Sie sich vom System ab- und erneut anmelden.

Sleex lässt sich zwar auch mit der Maus bedienen, eignet sich jedoch besser für eine Tastatursteuerung. Beim Drücken von [Super]+[F1] öffnet sich eine Tabelle mit den gängigsten verfügbaren Tastenkombinationen. Sie umfasst Shortcuts zur Navigation auf dem Desktop, für bestimmte Funktionsaufrufe und zum Start einiger Programme.

Dashboard

Sleex enthält ein Dashboard 3, das nicht nur wichtige Angaben zum System anzeigt, sondern auch das Ändern von Einstellungen und Aktualisieren des Systems ermöglicht. Darüber hinaus bietet es eine einfache Terminverwaltung. Die einzelnen Funktionen rufen Sie nach Kategorien sortiert in der Reiterleiste im oberen Fensterrand auf.

Das Einstellungsmenü bietet lediglich eine begrenzte Zahl von Optionen, die nicht mit den Konfigurationsmöglichkeiten anderer Arbeitsumgebungen vergleichbar sind. Detailliertere Anpassungen nehmen Sie in den jeweiligen Konfigurationsdateien vor. Dazu stellt der Hauptentwickler eine entsprechende Dokumentation bereit.

Calla

Der optionale Desktop Calla basiert auf dem Awesome Window Manager. Um diese Arbeitsoberfläche nach der Installation zu starten, wählen Sie im Login-Bildschirm unten links im Feld *Session* die Option *Calla* aus. Ansonsten startet der Awesome Window Manager, der durch sein rustikales Aussehen und die äußerst gewöhnungsbedürftige und veraltete Bedienung speziell auf Ein- und Umsteiger wohl eher abschreckend wirkt.

Zu bemängeln ist der noch unfertige Zustand des Desktops. Auf der Entwicklerseite von AxOS steht zu lesen, dass sich Calla bislang lediglich unter Debian installieren lässt. Die AxOS-Implementation ist zudem noch sehr lückenhaft. So gelingt es zum Beispiel nicht, viele der unter Sleex nutzbaren Werkzeuge aufzurufen, auch der Netzwerkzugang ließ sich im Test unter Calla nicht einrichten.

Calla arbeitet wie Sleex mit Tiling Windows und lässt sich ebenfalls per Tastatur bedienen. Entsprechende Belegungen finden Sie durch Drücken von [Super]+[F1] heraus. Bei Öffnen mehrerer Fenster werden diese teilweise nebeneinander oder in einem Raster geöffnet, wobei einige unter Umständen über die Arbeitsoberfläche hinausragen 4.

Die Panel-Leiste der Arbeitsumgebung am unteren Rand enthält rechts einen System-Tray und links ein Startmenü. Ein Klick auf eine der Statusanzeigen im Sys-

tem-Tray öffnet rechts auf dem Desktop zwei Fenster mit zusätzlichen Status- und Bedieninformationen 5. Darin aktivieren Sie unter anderem einen Medienabspieler und stellen die Lautstärke und die Bildschirmhelligkeit ein.

Auffällig ist der überraschend geringe RAM-Bedarf von nur 550 MByte im Leerlauf. Damit kommen selbst schwachbrüstige Systeme mit wenig Arbeitsspeicher zurecht. Die CPU-Belastung fällt ebenfalls sehr moderat aus.

Theom

Der auf dem Window-Manager i3 basierende Theom-Desktop lässt sich nicht während der Installation auswählen, sondern nur mithilfe der Paketverwaltung nachträglich installieren. Öffnen Sie dazu ein Terminal und geben Sie am Prompt das Kommando `epsi install theom` ein. Anschließend richtet die Routine die zusätzliche Arbeitsoberfläche ein.

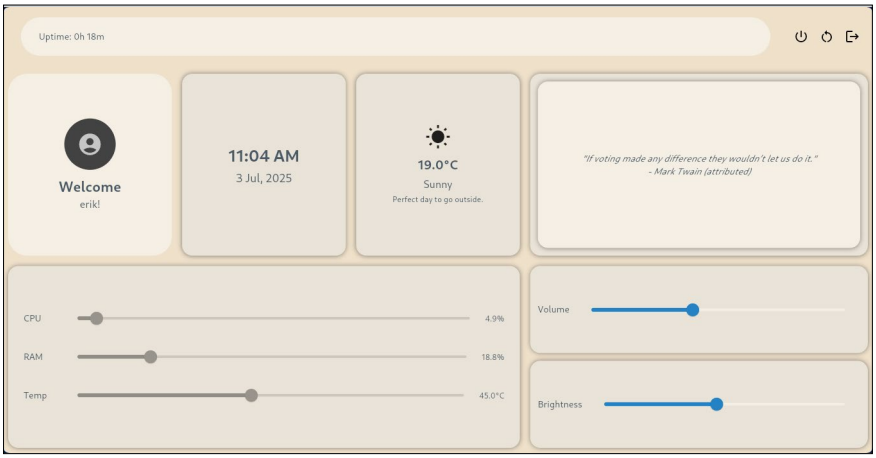
Beim nächsten Hochfahren wählen Sie im Login-Bildschirm unter *Session* unten links *Theom* als Benutzeroberfläche aus. Kurz darauf öffnet sich ein Assistent zur Konfiguration des Desktops. Mithilfe von *Customize theom appearance* wählen Sie aus einer Auswahl für die Anzeigeelemente auf der Arbeitsoberfläche eine Farbkombination aus. *View keybindings* erlaubt einen Blick auf die voreingestellten Tastenkombinationen. Der Theom zugrunde liegende Window-Manager i3 bietet wie Sleex und Calla eine Kachelansicht der Fenster 6.

Voreingestellt verfügt Theom über keinerlei auf dem Desktop sichtbaren Bedienelemente, Sie steuern den Desktop komplett über die Tastatur. Eine detailliertere Konfiguration nehmen Sie in der Datei `~/.config/theom/config.toml` vor, eine Dokumentation dazu stellt der Entwickler bereit.

Das voreingestellt aktivierte Dashboard zum Steuern der Grundfunktionen der Arbeitsoberfläche öffnen Sie mit [Super]+[Umschalt]+[D]. Darin sehen Sie neben der Auslastung wichtiger Systemkomponenten auch Datum und Uhrzeit sowie ein Wetter-Applet. Zudem stellen Sie hier die Lautstärke der Audioausgabe und die Bildschirmhelligkeit ein. Über drei Schaltknöpfe oben rechts melden Sie sich ab, fahren das System herunter oder starten es neu 7.

Fazit

AxOS fällt vor allem durch seine Vielfalt an schlanken Arbeitsumgebungen auf. Da das Projekt noch sehr jung ist, befinden sich diese Oberflächen aber noch in einem experimentellen Stadium. Produktiv lässt sich derzeit nur der Sleex-Desktop nutzen. Er zeigt, dass auch unter einer grafischen Oberfläche ein schnelles Arbeiten mit der Tastatur möglich ist, und bietet viele Anpassungsmöglichkeiten. Der geringe Ressourcenbedarf der Distribution macht sie auch für ältere PCs interessant. AxOS empfiehlt sich aktuell primär für experimentierfreudige Nutzer mit soliden Linux-Kenntnissen. (*tle*) ■



7 Das Dashboard gibt unter anderem Auskunft über die Systemressourcen und erlaubt das Steuern von Lautstärke und Bildschirmhelligkeit.

Weitere Infos und interessante Links
www.linux-user.de/qr/52463

Dateien zum Artikel herunterladen unter
www.linux-user.de/dl/52463

Grafische Managementlösungen für Docker

Einstiegshilfe

Docker gilt als eine der innovativsten Lösungen zur Containervirtualisierung. Mit komfortablen grafischen Verwaltungsoberflächen für Docker nutzen auch Einsteiger Containerumgebungen ohne längere Einarbeitung. Erik Bärwaldt

README

Obwohl Docker sich als führende Containerlösung auch im Heimbereich und kleinen Büros mehr und mehr etabliert, gibt es unter Linux nur wenige grafische Lösungen für das Verwalten kleinerer Docker-Installationen. Dieser Artikel stellt Docker Desktop, Portainer und Yacht vor, die einen schnellen Einstieg selbst in komplexere Docker-Umgebungen gestatten.

In professionellen IT-Infrastrukturen erfreuen sich Containerlösungen auf Basis von Docker im Vergleich zu herkömmlichen Virtualisierungsinstanzen zunehmender Beliebtheit. Die Vorteile von Docker-Containern liegen auf der Hand: Sie teilen sich den Kernel des Host-Systems, statt wie virtuelle Server jeweils ein komplettes Betriebssystem zu benötigen. Das macht Container wesentlich kompakter, und auch ihre Konfiguration fällt im Vergleich zu gängigen virtuellen Maschinen wesentlich leichter.

Zudem skalieren Containerlösungen deutlich besser als virtuelle Maschinen und benötigen weniger Ressourcen. Sie lassen sich dank der gekapselten Images einfach aufsetzen, und auf einer einzigen Betriebssysteminstanz können mehrere Docker-Anwendungen simultan laufen. Durch die Kapselung der einzelnen Container ist es darüber hinaus möglich, ihnen individuell Ressourcen des Host-Systems zuzuweisen.

Doch mit der steigenden Komplexität der Containersysteme wird auch ihre Verwaltung schwieriger. Grafische Oberflächen für Docker-Container versprechen, das Handling der Systeme zu vereinfachen und so selbst ambitionierten Heimanwendern und Nutzern in kleinen Organisationen die Vorteile von Docker unmittelbar näherzubringen. Wir werfen daher im Folgenden einen genaueren Blick auf die wichtigsten grafischen Werkzeuge zum Docker-Management.

Anforderungen

Damit sich grafische Frontends zur Verwaltung von Docker-Containern flexibel einsetzen lassen, sollten sie neben dem reinen Management der Docker-Systeme einige zusätzliche Funktionen bieten. Idealerweise arbeitet das jeweilige Frontend als webbasierte Applikation, damit man es auch auf entfernten Maschinen nutzen kann. Zudem sollte es statistische Angaben liefern, die es ermöglichen, Systemressourcen individuell zuzuweisen. Derartige Informationen können über-

dies beim Beheben von Problemen helfen, sofern sich die Log-Dateien innerhalb des Frontends einsehen lassen. Dabei muss eine Übersicht über alle bestehenden Container gewährleistet bleiben, und zwar ganz unabhängig von ihrem aktuellen Betriebszustand.

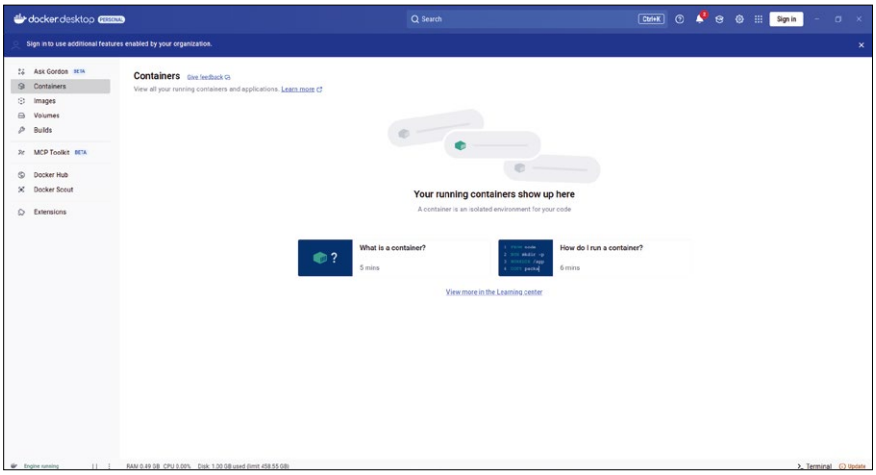
Docker Desktop

Die Webseite von Docker offeriert als offizielles grafisches Frontend zur Containervirtualisierung das aus dem Werkzeug Kitematic hervorgegangene Docker Desktop. Die plattformübergreifend erhältliche grafische Managementlösung für Docker-Umgebungen nutzt unter Linux eine virtuelle Maschine als Laufzeitumgebung. Sie erzeugt einen eigenen Docker-Kontext, weshalb Container und Images, die zuvor mithilfe der Linux Docker Engine aufgesetzt wurden, nicht in Docker Desktop erscheinen.

Das Tool arbeitet ausschließlich auf 64-Bit-Betriebssystemen, setzt Systemd voraus und benötigt zur Virtualisierung KVM sowie Qemu in Version 5.2 oder neuer. Es benötigt mindestens 4 GByte Arbeitsspeicher im System. Als Desktop-Umgebung empfehlen die Entwickler KDE Plasma, Gnome oder Mate.

Weil Docker Desktop zahlreiche weitere Anwendungen integriert, darunter Kubernetes (K8s), Docker Compose und die Docker-Engine, können Sie ohne aufwendige Einzelinstallationen schnell eine aktuelle Docker-Umgebung aufsetzen. Die ausgezeichnete englischsprachige Dokumentation legt alle wichtigen Installationsschritte und die Nutzung des grafischen Frontends ausführlich dar.

Privatanwender oder kleine Unternehmen können das Docker-Desktop-Paket kostenfrei einsetzen, größere Organisationen müssen hingegen eine Lizenz erwerben. Die enthält allerdings auch spezielle Funktionen wie den Hardened Docker Desktop, der sicherheitsbewussten Administratoren eine spezielle Rechteverwaltung für die Anwender ermöglicht und Container in gesondert abgeschotteten Umgebungen betreibt. Derartige Funktionen fehlen in der Community-Variante. Die kostenpflichtigen Versionen umfassen zudem Support-Pakete, und es kann mehr als ein Benutzer die Containerumgebung nutzen.

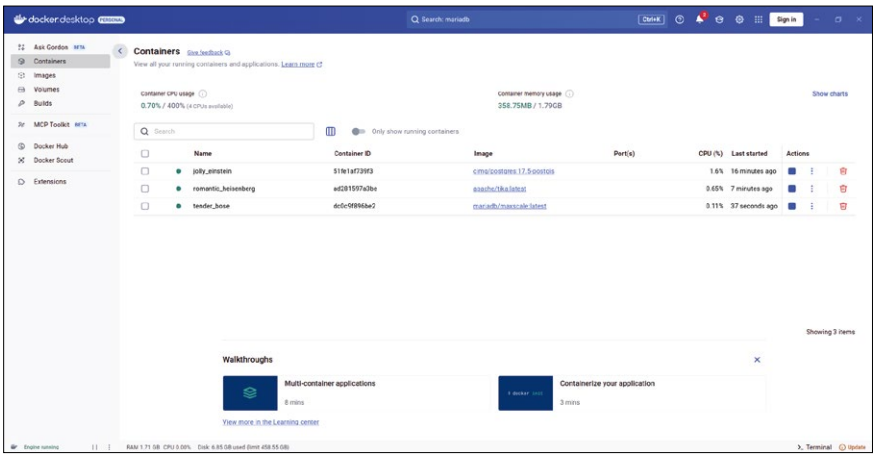


1 Docker Desktop bietet einen sofortigen Einstieg in die Welt der Container.

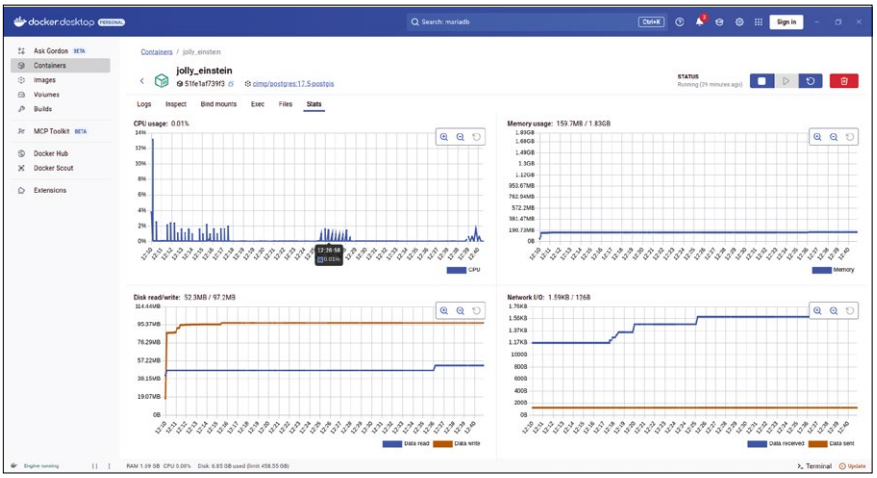
Installation

Bei der Installation halten Sie sich am besten strikt an die offizielle Anleitung. Haben Sie alle Vorarbeiten erledigt, installieren Sie anhand der Dokumentation das jeweils zwischen rund 350 und 380 MByte umfassende Paket.

Beachten Sie bitte, dass die offiziellen Releases lediglich Debian, Ubuntu, Fedora und Red Hat Enterprise Linux (RHEL) in den Versionen 8 und 9 unterstützen. Bei der Integration in eine RHEL-Instanz muss zudem ein Docker-Konto vorhanden sein. Die Debian-Variante unterstützt lediglich das aktuelle Debian 12 „Bookworm“ in der 64-Bit-Version. Bei Ubuntu muss eine der beiden letzten LTS-Varianten oder die aktuelle Version 25.04 ohne LTS-Support vorhanden sein.



2 Die im System vorhandenen Images zeigt Docker Desktop übersichtlich an.



3 Docker Desktop bringt auch eine containerspezifische Statistikfunktion mit.

Nicht berücksichtigt

Neben den besprochenen Kandidaten gibt es unter Linux etliche weitere Werkzeuge zur Administration von Docker-Umgebungen. Einige davon werden jedoch nicht mehr weiterentwickelt, wie DockStation (letztes Release 2019), Shipyard (2016) und DockerUI (ebenfalls 2016). Bei Lazydocker und Docui handelt es sich um Terminalanwendungen. Während Lazydocker nach wie vor aktiv ist, wurde Docui bereits 2019 eingestellt.

Docker Desktop ist keine webbasierte Anwendung, sondern auf das jeweilige Computersystem beschränkt. Durch einen Klick auf den Starter in der Menüstruktur öffnen Sie nach dem Bestätigen der Lizenzbedingungen ein übersichtliches, zweigeteiltes Dashboard. Im rechten Segment werden dabei Docker-Container angezeigt 1. In diesem Bereich befinden sich beim ersten Start lediglich zwei Assistenten. Links finden Sie in einer vertikalen Steuerleiste verschiedene Gruppen wie *Containers*, *Images*, *Volumes* und *Builds*, über die Sie die aktuellen Statusanzeigen der jeweiligen Komponenten einblenden. Dazu gehören beispielsweise Angaben zum Speicherbedarf sowie der CPU- und RAM-Auslastung, die ganz unten horizontal in einer Leiste in den jeweiligen Anzeigen erscheinen. Mit *Ask Gordon* steht außerdem ein KI-Assistent zur Verfügung, der sich allerdings noch im Beta-Stadium befindet.

Konfiguration

Zur Konfiguration von Docker Desktop klicken Sie auf das Zahnradsymbol oben rechts im Dashboard und gelangen so in die Einstellungsdialoge. Für Administratoren größerer Docker-Umgebungen ist besonders die über die Gruppenleiste links erreichbare Option *Resources* interessant. Hier legen Sie fest, mit wie vielen CPU-Kernen Docker arbeiten darf.

Außerdem definieren Sie mithilfe von Schiebereglern die zur Verfügung stehende Arbeitsspeicherkapazität sowie die Größe des Swap-Speichers und die maximal nutzbare Kapazität des Massenspeichers. In der Gruppe *Kubernetes* legen Sie außerdem fest, ob beim Aufruf von Docker Desktop auch K8s im Single- oder Multi-Node-Modus startet. So binden Sie die Orchestrierungslösung nahtlos in Docker Desktop ein.

In der Kategorie *Beta features* nehmen Sie gegebenenfalls Funktionen in die Installation auf, die sich noch in der Entwicklung befinden. Diese Funktionen integrieren Sie jeweils durch Setzen eines Häkchens ins System. Da die Beta-Funktionen noch Fehler enthalten können, sollten Sie sie in produktiven Umgebungen nicht einsetzen.

Aufrüsten

Um der Installation neue Docker-Images und Container hinzuzufügen, benutzen Sie die Suchfunktion, die Sie oben im Dashboard finden. In einem gesonderten Fenster geben Sie den Namen der gewünschten Anwendung ein und erhalten dann eine Liste der verfügbaren Images. Daraus wählen Sie das gesuchte Abbild aus und klicken auf den Button *Run* rechts daneben. Die Routine lädt nun das Image herunter und öffnet ein weiteres kleines Fenster, in dem Sie Optionen für den neuen Container angeben. Anschließend klicken Sie erneut auf *Run*, woraufhin das Tool den Container generiert und in der Containerübersicht anzeigt.

Steuerung

Die Spalte *Actions* rechts neben jedem Container-, Image- oder Volume-Eintrag dient der Steuerung der einzelnen Docker-Komponenten. Sie enthält je nach Kontext verschiedene Symbole. In allen drei Kategorien finden Sie einen Papierkorb, der es ermöglicht, die entsprechende Komponente aus dem System zu entfernen. Dabei werden beim Löschen von Containern auch alle zugehörigen Volumes komplett aus der Instanz entfernt.

Durch einen Mausklick auf das Stopp-Symbol deaktivieren Sie den betreffenden Container. Einen Neustart oder ein Pausieren sowie einige weitere Aktionen zur lückenlosen Überwachung einer Komponente finden Sie im Punkte-Menü in der Rubrik *Actions*. Ein Klick auf das

blaue Start-Symbol links daneben aktiviert den jeweiligen Container.

Inaktive Images starten Sie analog, indem Sie in der Gruppe *Images* rechts in der Spalte *Actions* auf das Start-Symbol klicken. In der Statusleiste erscheint in der Containeransicht zusätzlich die Anzeige der Prozessor- und Arbeitsspeicherauslastung, wobei das Tool die Beanspruchung der CPU für jeden Container gesondert ausweist 2. Mithilfe des Papierkorbs löschen Sie deaktivierte Images, sofern der dazugehörige Container bereits entfernt wurde.

Zusatzfunktionen

Docker Desktop führt für jeden Container eigene Log-Dateien. Über ein integriertes Terminal können Sie spezifische Funktionen kontextsensitiv auslösen. Außerdem lassen sich statistische Daten zu jedem Container abrufen und Umgebungsvariablen prüfen.

Um diese Funktionen zu nutzen, klicken Sie in der Kategorie *Containers* auf den gewünschten Eintrag in der Listenansicht. Im Hauptsegment des Fensters öffnet sich nun ein Bereich mit den Reitern *Logs*, *Inspect*, *Bind mounts*, *Exec*, *Files* und *Stats*. Im aktivierten Reiter *Logs* sehen Sie die Protokolle des jeweiligen Containers durch und lokalisieren so eventuelle Probleme. Im Reiter *Exec* finden Sie das interne Terminal, in dem Sie für den Container spezifische Befehle ausführen. Der Reiter *Stats* öffnet eine grafische Ansicht zum Ressourcenbedarf des Containers, sodass Sie Unregelmäßigkeiten sofort erkennen 3.

Extensions

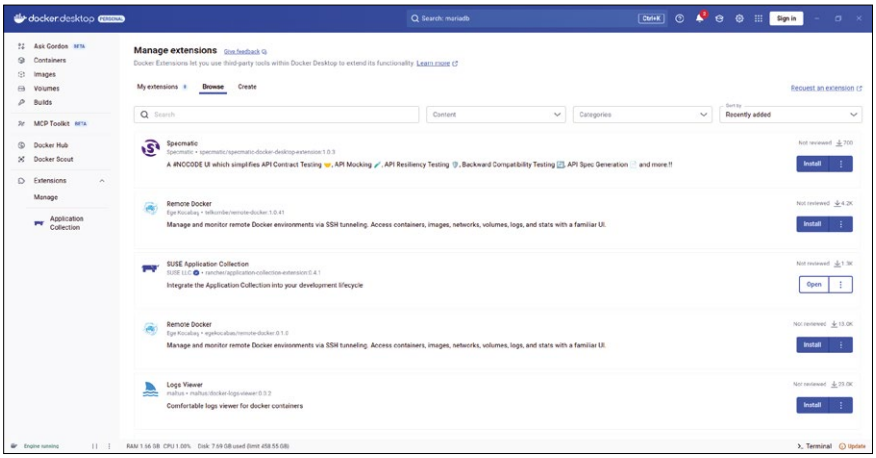
In der Kategorie *Extensions* integrieren Sie Erweiterungen in Docker Desktop. Nach einem Klick auf diese Rubrik öffnet sich der Reiter *Browse* mit einem Browser, in dem Sie die gewünschte Erweiterung auswählen. Danach klicken Sie auf *Install* rechts daneben. Die neue Funktion taucht daraufhin in der linken Steuerleiste unter dem Eintrag *Extensions* auf. Dort können Sie sie durch Anklicken ausführen. Installierte Erweiterungen erscheinen zudem in der Kategorie *Images* und lassen sich wie jedes beliebige andere Image verwalten 4.

Portainer

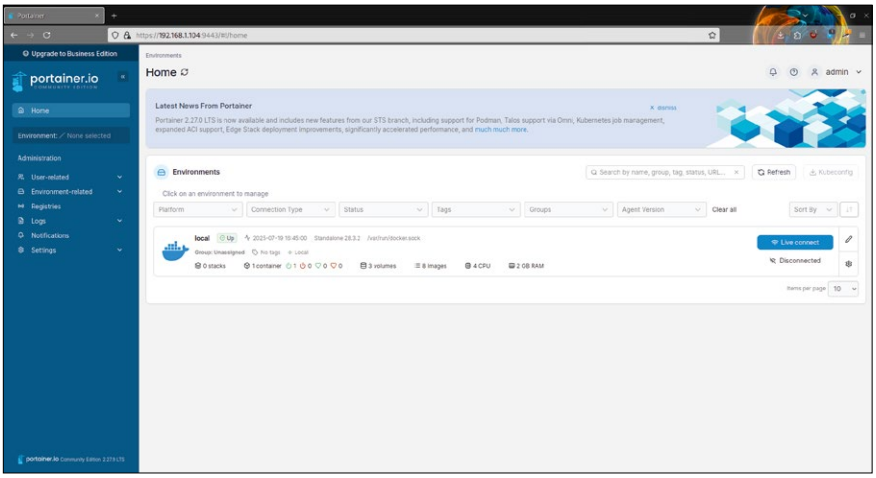
Die webbasierte Anwendung Portainer zielt primär auf das Verwalten von Cluster-Infrastrukturen ab. Damit lassen sich beispielsweise Kubernetes-Deployments unter einer einheitlichen Bedienoberfläche steuern. Quasi nebenläufig erleichtert Portainer signifikant das Verwalten von Docker-Containern. Die Anwendung lässt sich nicht nur in lokalen Infrastrukturen einsetzen, sondern harmoniert auch mit Cloud-Umgebungen.

Die Software umfasst zwei Komponenten: Während der Portainer-Server als Datenbank lokale Docker-Instanzen verwaltet, sind Portainer-Agenten primär für Cluster-Umgebungen konzipiert. Sie benötigen jedoch auch für Standalone-Infrastrukturen jeweils einen Agenten. Auf den einzelnen Cluster-Knoten arbeitet ebenfalls ein Portainer-Agent. Die Installation des Portainer-Servers setzt eine bereits laufende Docker-Infrastruktur voraus, da die Applikation selbst als Docker-Image vorliegt. Sie lässt sich sogar via Docker Desktop einrichten.

Wie Docker Desktop liegt auch Portainer in einer kostenfreien und quelloffenen Community-Edition sowie in mehreren kostenpflichtigen Business-Varianten vor. Letztere verfügen über diverse, speziell für Mission-Critical-Umgebungen relevante Sonderfunktionen, die erhöhte Sicherheitsanforderungen besser unterstützen. Zur Installation von Portainer mit Docker unter Linux findet sich eine ausführliche Dokumentation auf der Webseite des Projekts.



4 Über Erweiterungen binden Sie zusätzliche Funktionen in das System ein.

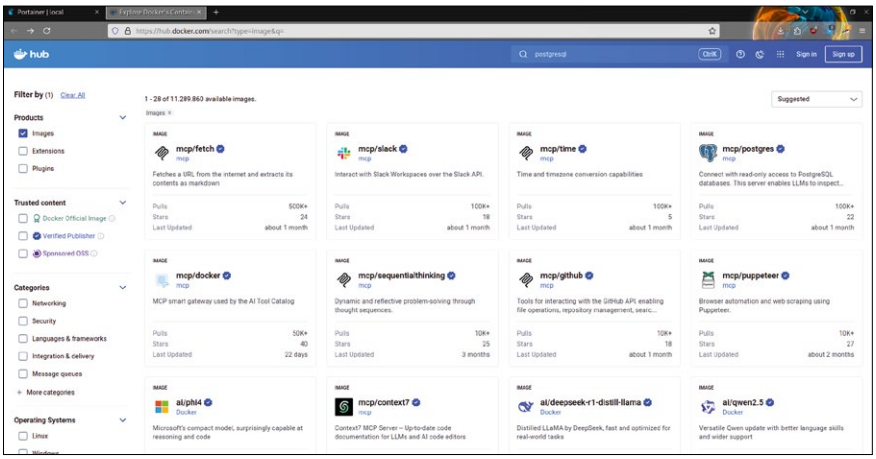


5 Portainer unterstützt die Inbetriebnahme mit einem eigenen Assistenten.

Nutzung

Nach der Installation läuft Portainer mit allen Zusatzkomponenten als Docker-Container und lässt sich sofort von jeder Arbeitsstation im LAN aus über die URL https://*IP-Adresse*:9443 in einem beliebigen Webbrowser ansprechen. Beim ersten Aufruf legen Sie noch ein Passwort für den administrativen Zugang (Nutzer *admin*) fest, das mindestens 12 Zeichen umfassen muss.

Danach gelangen Sie in die Portainer-Oberfläche, in der Sie zunächst einen Assistenten für den Schnelleinstieg starten. Darin wählen Sie im ersten Schritt die lokale Docker-Umgebung aus und erhalten anschließend im Dashboard in einem gesonderten Fenstersegment statistische Daten dazu angezeigt 5.



6 Auf Docker Hub finden Sie zahlreiche Images, die sich direkt einbinden lassen.

Konfiguration

Portainer bietet umfangreiche Einstellungsmöglichkeiten. Dazu gehört unter anderem eine Nutzerverwaltung, die auch Rollen für die einzelnen Anwender und Gruppen (*Teams*) umfasst. Die Konfigurationsdialoge erreichen Sie über die Leiste, die sich links im Dashboard befindet, in der Gruppe *Settings*.

Neben nutzungsspezifischen Einstellungen finden sich hier in mehreren Unterkategorien diverse Optionen zur Programmsteuerung. Darin legen Sie jeweils in eigenen Dialogen fest, wie Portainer Backups behandeln soll und wie häufig es Snapshots anlegt. Sicherheitsspezifische Anpassungen wie die Integration von SSL-Zertifikaten oder Konfigurationsänderungen beim Einsatz von Kubernetes nehmen Sie ebenfalls an dieser Stelle vor.

Docker-Management

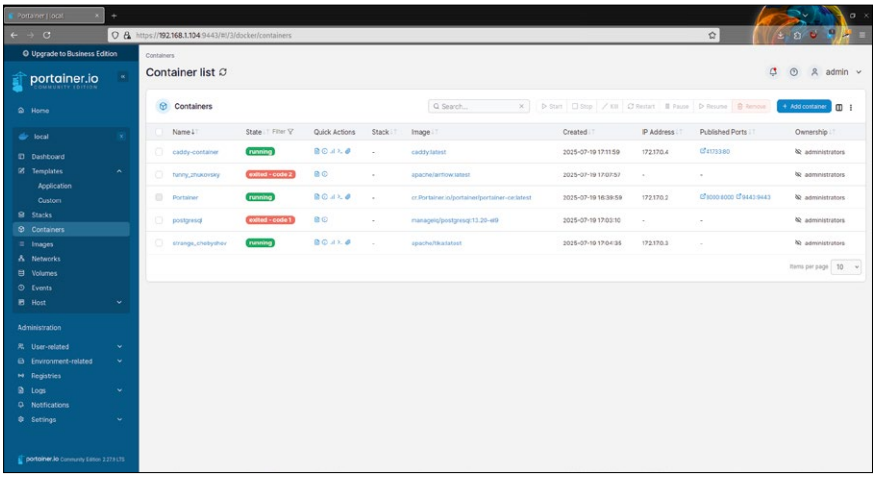
Die eigentliche Verwaltung der Docker-Umgebung erledigen Sie wie in Docker Desktop in unterschiedlichen Kategorien, die eine Leiste links im Fenster untereinander aufführt. Zunächst verbinden Sie im Übersichtsbereich *Home* im Segment *Environments* die lokale Docker-Umgebung mit der Portainer-Instanz, indem Sie rechts auf die blaue Schaltfläche *Live connect* klicken.

Die bereits vorhandenen Volumes, Images und Container können Sie nun sofort einsehen, indem Sie dort die gleichnamigen Kategorien aufrufen. In allen Kategorien zeigt Portainer die bereits installierten Komponenten an, wobei die Containertabelle den Status der einzelnen Container signalisiert. In der Spalte *Quick Actions* führen Sie verschiedene Aktionen im Schnellzugriff aus. So gestattet beispielsweise ein bei jedem Container vorhandener Link die Einsicht in die jeweilige Log-Datei.

Die oberhalb der Containertabelle befindliche Schalterleiste dient der Steuerung der einzelnen Container. Um einen Container hinzuzufügen, klicken Sie oben rechts auf *Add container*. Sie gelangen in einen Einstellungsdialog, in dem Sie zunächst einen Namen für den neuen Container vergeben. Danach legen Sie in der Zeile *Image* das zugehö-

rige Image fest, das Sie von Docker Hub beziehen möchten. Über *Search* können Sie dabei in einem gesondert geöffneten Reiter im Webbrowser die Image-Liste durchsuchen und anhand von Kategorien vorsortieren 6. Nach der Eingabe des Image-Namens klicken Sie im einfachsten Fall weiter unten auf den blauen Button *Deploy the container*. Im Abschnitt *Advanced container settings* finden Sie bei Bedarf verschiedenste Konfigurationsmöglichkeiten.

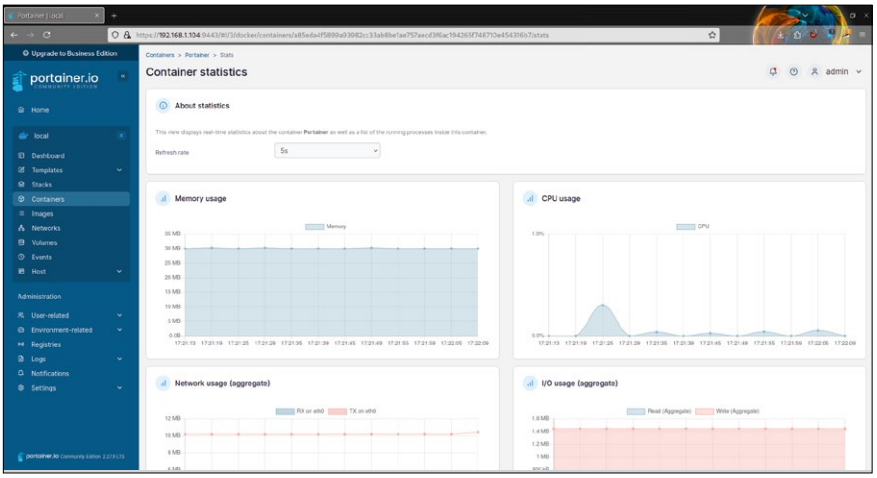
Eine weitere Möglichkeit, Container bequem in das System einzufügen, bietet die Option *Templates* links in der Kategorienleiste. Ein Klick darauf öffnet rechts eine Liste mit vorhandenen Vorlagen. Durch Anwählen einer davon gelangen Sie in einen Einstellungsbildschirm, in dem Sie bei Bedarf noch individuell Optionen anpassen können. Anschließend klicken Sie erneut auf *Deploy the container*. Je nach gewählter App dauert es nun eine Weile, bis Portainer das Image heruntergeladen und den Container in Docker integriert und gestartet



7 Portainer zeigt auf einen Blick den Status der vorhandenen Container.

hat. Anschließend springt das Tool in die Ansicht *Containers* und führt den neuen Container an erster Stelle auf 7.

Um einen Container zu entfernen, markieren Sie ihn, indem Sie links neben der Namensspalte ein Häkchen setzen. Anschließend klicken Sie oben rechts in



8 Mit einer ebenso übersichtlichen wie aussagekräftigen Monitoring-Funktion veranschaulicht Portainer den Ressourcenbedarf der einzelnen Container.

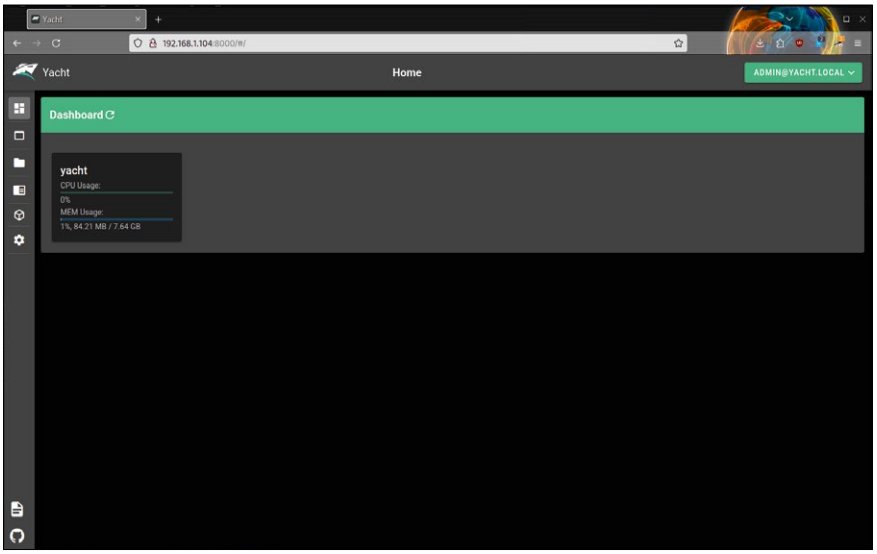
der Schalterleiste auf *Remove*. Nach einer Sicherheitsabfrage entfernt Portainer den Container aus der Docker-Umgebung. Um mehrere Container gleichzeitig zu entfernen, gehen Sie analog vor und markieren in einem Durchgang alle zu entfernenden Container durch Setzen eines Häkchens. Möchten Sie andere Steuerelemente eines Containers verwenden, müssen Sie ihn ebenfalls zuvor durch Setzen eines Häkchens markieren. Das aktiviert in der Schalterleiste oberhalb der Containertabelle alle Steuerelemente, die sich auf den markierten Container anwenden lassen. Den laufenden Container von Portainer selbst können Sie weder stoppen noch pausieren, da sonst die Verwaltungsoberfläche nicht mehr verfügbar wäre.

Wenn Sie zwei oder mehr Container für den gemeinsamen Einsatz in einem Stack zusammenfassen möchten, nutzen Sie dazu die Kategorie *Stacks*. Nach einem Klick auf *Add stack* oben rechts geben Sie in einem sich öffnenden Webeditor die zum Anlegen des Stacks nötigen Befehle ein. Anschließend klicken Sie unten links auf *Deploy the stack*, woraufhin Portainer ihn erzeugt und in die Liste der Stacks aufnimmt. Jetzt taucht der Stack auch im Dashboard auf.

Logs und Statistik

In der Containerliste finden Sie in der Spalte *Quick Actions* verschiedene Symbole für den Schnellzugriff auf häufig benötigte Ressourcen. Unter anderem öffnen Sie hier mit einem Klick auf das Büroklammersymbol ganz rechts eine Konsole zur Befehlseingabe. Ein Klick auf das Papierblatt-Symbol ganz links öffnet ebenfalls eine Konsole, die allerdings nur der Anzeige der Log-Informationen dient. Mit deren Hilfe grenzen Sie bei Bedarf auftretende Probleme ein, ohne dazu Portainer verlassen und in einem externen Terminal arbeiten zu müssen.

Mittig in der Spalte *Quick Actions* finden Sie für jeden laufenden Container ein Balkengrafiksymbol. Ein Klick darauf öffnet eine aussagekräftige und dennoch übersichtliche grafische Ansicht zu den verschiedenen Ressourcen, die der jeweilige Container für sich beansprucht 8. Nahezu in Echtzeit sehen Sie hier die Prozessorlast, den RAM-Bedarf, das Traffic-Volumen sowie in einer Tabellenansicht die im aktuellen Container arbeitenden Prozesse. Diese Tabellen können im Fall von Problemen oder inkonsistenten Funktionen des Containers Hinweise auf die Fehlerquelle liefern. Die Aktualisierungsfrequenz der Ansichten modifizieren Sie bei Bedarf oberhalb der Graphen im Feld *Refresh rate*.



9 Yacht präsentiert nach dem ersten Start eine sehr spartanisch wirkende Oberfläche.

Yacht

Das grafische Docker-Frontend Yacht möchte den Umgang mit Docker-Containern so einfach wie möglich gestalten. Dazu setzt es vornehmlich auf Templates,

die sich per Mausklick in eine Docker-Umgebung integrieren lassen. Dabei ist Yacht zu Portainer kompatibel, sodass Sie beide parallel installieren und nutzen können. Yacht ermöglicht außerdem das Editieren von Containern und bietet daneben ein Dashboard zum Monitoring. Routinen zur Nutzerverwaltung und ein Interface für die Kommandozeile fehlen der Software derzeit noch.

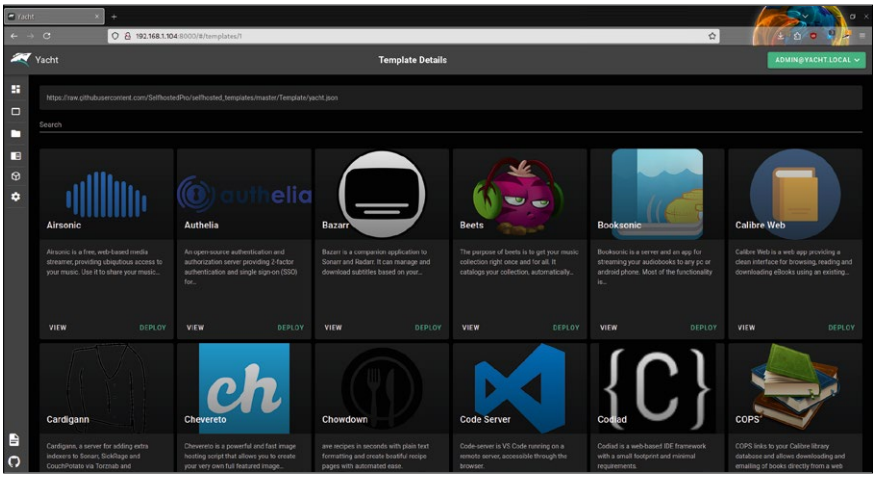
Unter Linux kommt Yacht mit den Architekturen x86_64 und ARM zurecht, für den Raspberry Pi gibt es Pakete für die ARMv7- sowie die ARM64-Modelle. Andere Betriebssysteme unterstützt Yacht nicht. Softwareseitig setzt das Tool nur eine aktive Docker-Instanz voraus. Auf der neuen, noch im Aufbau befindlichen Projektseite finden Sie eine kleine Anleitung zur Installation via Docker, klassische Pakete gibt es nicht. Daneben beschreibt die Anleitung alternative Methoden wie die Installation über OpenMediaVault oder über Docker Compose. Sie fallen jedoch komplizierter aus und bedürfen manueller Eingaben. Da das Programm webbasiert arbeitet, wird der entsprechende Docker-Container bei der Installation fertig vorkonfiguriert.

Inbetriebnahme

Im Webbrowser des Docker-Systems rufen Sie die Oberfläche von Yacht über die URL http://*IP-Adresse*:8000 auf. Läuft auf dem System bereits eine Instanz von Portainer, verwenden Sie anstelle des Ports 8000 den Port 8001. Sie gelangen in einen Login-Bildschirm, in dem Sie sich mit der E-Mail-Adresse admin@yacht.local und dem Passwort pass anmelden. Daraufhin öffnet sich eine etwas spartanisch aussehende Oberfläche, in der das Dashboard lediglich einen einzigen Eintrag enthält 9.

Die Bedienelemente zur Administration des Docker-Systems finden Sie in Form kleiner Icons in einer vertikal am linken Fensterrand angeordneten Steuerleiste. Im ersten Schritt empfiehlt es sich, oben rechts auf den grünen Schalter mit der E-Mail-Adresse des Administrators zu klicken und im sich öffnenden Kontextmenü die Option *User* auszuwählen.

Im jetzt erscheinenden Einstellungsdialog modifizieren Sie über die Option *Change Password* oben links die Zugangsdaten. Nach Eingabe einer E-Mail-Adresse und eines neuen Passworts klicken Sie unten rechts auf *Change User Info*. Wenn Sie danach den Mauszeiger über eines der Icons in der Steuerleiste bewegen, klappt das Menü auf, das die Namen der einzelnen Symbole anzeigt.



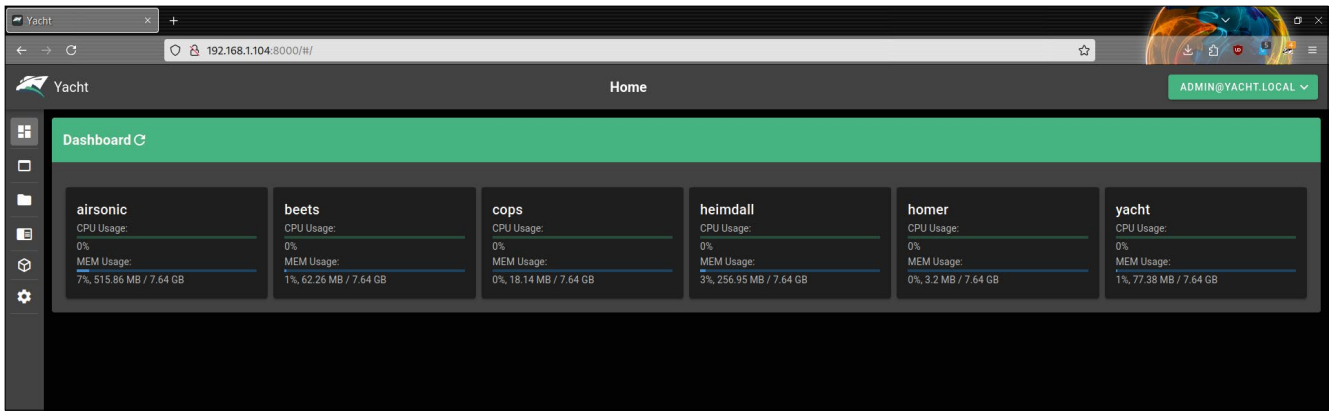
10 Yacht wartet mit zahlreichen vorkonfigurierten Templates auf.

Container hinzufügen

Um dem lokalen System Container aus der vorhandenen Template-Liste hinzuzufügen, wählen Sie links in der Steuerleiste den Eintrag *Templates*. Im sich daraufhin öffnenden Fenstersegment klicken Sie rechts neben dem Titel *Templates* auf das Pluszeichen. Sie gelangen nun in einen Eingabebereich, in dem Sie einen Titel und eine URL für die neue Vorlage eingeben müssen.

Die auf Github vorhandene Template-Liste sehen Sie ein, indem Sie die oben im Fenster angegebene URL kopieren und in die entsprechende Eingabezeile einfügen. Danach klicken Sie darunter auf *Submit*. Die Software springt nun zurück in die Template-Anzeige und listet hier als ersten Eintrag die soeben angelegte Vorlage auf. Ein Doppelklick darauf blendet danach die Liste aller auf Github vorhandenen Templates ein, wobei Yacht jeweils eine kurze Beschreibung dazu anzeigt 10.

Zum Erzeugen eines Containers klicken Sie unterhalb der Beschreibung des jeweiligen Templates auf *Deploy*. Sie gelangen anschließend in einen Einstellungsbildschirm, in dem die wesentli-



11 Das Dashboard von Yacht zeigt alle Container inklusive ihrer Statusdaten an.

chen Optionen bereits konfiguriert sind. Ein Mausklick auf *Continue* führt Sie in den nächsten Konfigurationsbildschirm, der ebenfalls mit sinnvollen Voreinstellungen aufwartet.

Am oberen Rand des Einstellungsdialogs finden Sie eine Leiste, die anzeigt, wie viele Dialoge es zum Anpassen des Containers zu durchlaufen gilt. Dabei kennzeichnet ein grüner Punkt den aktuell geöffneten Dialog. Mit einem Klick auf *Continue* wechseln Sie jeweils in den nächsten Dialog. Bei Erreichen des letzten Dialogs erscheint stattdessen der Schalter *Deploy*, mit dem Sie den komplett eingestellten Container aktivieren. Während des folgenden Herunterladens des Templates aus dem Internet signalisiert ein Laufbalken am oberen Rand des Dialogs den Fortschritt.

Anschließend springt die Anzeige in die Kategorie *View Applications* und listet die neue Anwendung mit einigen statistischen Daten auf. Die *Apps*-Anzeige entspricht dabei der Containeransicht von Portainer oder Docker Desktop. In der Kategorie *Resources* | *Images* finden Sie das zum neu angelegten Container gehörige Image. Die Unterkategorie *Volumes* führt die vorhandenen Volumes auf.

In der *Apps*-Ansicht können Sie die vorhandenen Container auch steuern. Dazu finden Sie links neben jeder Containerbezeichnung ein kleines offenes Dreieck. Ein Klick darauf öffnet jeweils ein Kontextmenü mit allen gängigen Steuerelementen. Bei Bedarf rufen Sie über den Punkt *Edit* den ursprünglichen Konfigurationsdialog erneut auf und nehmen dort Anpassungen an den Einstellungen des Containers vor. Sie durchlaufen dabei alle Einrichtungsdialoge und klicken abschließend wieder auf *Deploy*, um den Container zu modifizieren.

Im Dashboard zeigt Yacht anschließend alle installierten Container samt Daten zu den wichtigsten Betriebsparametern in Kachelform an 11. So erkennen Sie auf einen Blick, ob die Container alle erwartungsgemäß arbeiten.

Fazit

Obwohl Docker sich mehr und mehr als führende Containerlösung etabliert, gibt es unter Linux kaum grafische Lösungen für das Verwalten kleinerer Docker-Installationen. Doch die drei hier besprochenen Anwendungen erfüllen ihren Zweck bestens und gestatten einen schnellen Einstieg selbst in komplexere Docker-Umgebungen. Alle bieten eine hervorragende Dokumentation, die Einsteiger Schritt für Schritt zu einer funktionierenden Docker-Instanz mit dem jeweiligen grafischen Frontend führt.

Docker Desktop fällt dabei etwas aus dem Rahmen, da es unter Linux als native Anwendung einer gesonderten Installation bedarf. Portainer hat da als webbasierte, im lokalen Netz universell einsetzbare Lösung eindeutig die Nase vorn. Für Einsteiger eignet sich am ehesten Yacht, da diese Applikation ohne größere Einarbeitung sofort das Management kleinerer Docker-Umgebungen zulässt. Eine Nutzerverwaltung würde den Einsatzbereich von Yacht flexibler gestalten und befindet sich nach Angabe des Projekts bereits in Arbeit. (*jlu*)

Weitere Infos und interessante Links

www.linux-user.de/qr/51496

PROBELESEN OHNE RISIKO

TESTEN SIE JETZT 3 AUSGABEN FÜR 19 €

OHNE DVD 15 €

amazon

5 EURO-GUTSCHEIN

Abo-Vorteile

42% Rabatt

- Günstiger als am Kiosk
- Versandkostenfrei bequem per Post
- Pünktlich und aktuell
- Keine Ausgabe verpassen

SICHERN SIE SICH JETZT IHR GESCHENK!

EIN AMAZON-GUTSCHEIN ÜBER 5,00 €

- Telefon: 0911 / 993 990 98
- E-Mail: computec@dpv.de

Einfach bequem online bestellen: shop.linuxuser.de

Auf Nummer sicher: OpenSuse-Systeme zusätzlich gegen Angriffe härten

Sicherheitskontrolle

Linux gilt als weitgehend sicher, aber Sorglosigkeit ist dennoch gefährlich. Die Sicherheit eines OpenSuse-Systems lässt sich gegenüber dem Auslieferzustand verbessern.

Peter Kreußel

README

OpenSuse-Anwender vertrauen in der Regel darauf, dass ihnen ihre Distribution ein sicheres Gesamtpaket liefert. Dennoch lässt sich die Sicherheit eines OpenSuse-Systems gegenüber dem Auslieferungszustand mit einigen Handgriffen noch optimieren.

Die Linux-Kernel-Entwickler um Linus Torvalds liefern einen stabilen, professionell aktuell gehaltenen Systemkern. Linux-Anwender haben seltener mit ungebetenen Gästen zu kämpfen als ihre Windows-Kollegen, wozu allerdings auch die geringe Verbreitung beiträgt. Im Vergleich zur schieren Anzahl der von Laien oft mehr schlecht als recht gewarteten Windows-Installationen bleibt Linux ein Exot. Zudem gibt es nicht das eine Linux. Die Distributionen differieren in den Versionsständen der Software, sodass Angriffstechniken oft nur für eine geringe Anzahl von Rechnern funktionieren.

Doch auch unter Linux hängt viel vom umsichtigen Verhalten der Anwender ab: Das sicherste System nutzt wenig, wenn ein Login aus dem Internet mit einem leicht zu erratenden Passwort möglich ist. Zudem weist auch Linux-Software oft genug Sicherheitslücken auf, wenngleich sie dank des Open-Source-Prinzips oft schneller entdeckt und beseitigt werden. Sich auf die Grundsicherheit von Linux und der Router-Firewall 1 zu verlassen, geht zwar meist lange gut, aber eben auch nicht immer.

Vertrauenskette

Wer unter Linux Software installiert, vertraut auf zweierlei: Dass sein Distributor die Sicherheit im Auge behält und sich bei Bekanntwerden von Lücken zügig um Fixes kümmert. Hinter OpenSuse steht die im Enterprise-Umfeld erfolgreiche Firma Suse. Ein guter Teil der Pakete in Leap entstammt direkt der Enterprise-Distribution SLES des Unternehmens und erbt damit deren Sicherheit.

Die auf dem Suse-spezifischen Libzypp basierende Softwareverwaltung garantiert per Signatur, dass die Pakete trotz Übertragung über das unsichere Medium Internet in unkompromittierter Form beim Anwender ankommen. Voraussetzung ist, dass die Schlüssel, anhand derer Zypper die Pakete prüft, authentisch sind. Die originalen OpenSuse-Keys stammen ursprünglich vom Installationsmedium, dessen Unverfälschtheit sich

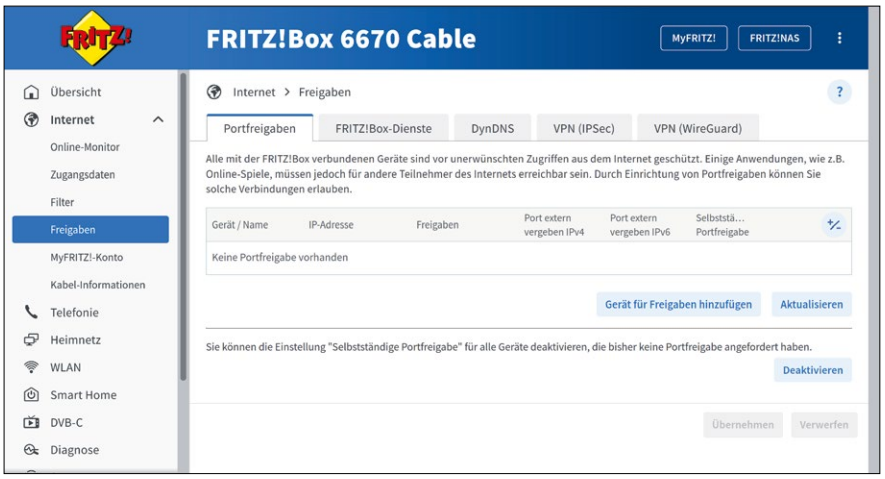
anhand von Prüfsummen verifizieren lässt 2. Die Paketverwaltung fragt beim Einbinden neuer Paketquellen stets beim Benutzer nach, ob sie dem Repository-Schlüssel vertrauen soll 3.

Es kostet nur wenig Mühe, die in der Paketverwaltung hinterlegten Schlüssel mit den im Internet veröffentlichten Schlüssel-Fingerprints abzugleichen. Das auf GPG-Technik setzende Verfahren garantiert, dass sich Schlüssel mit einem gegebenen Fingerprint nicht gezielt erzeugen lassen. Stimmen die lokalen Fingerprints mit den online recherchierbaren Versionen überein, können die Anwender davon ausgehen, dass die Schlüssel unverfälscht sind.

Alle von der Paketverwaltung genutzten Schlüssel lassen sich im YaST-Modul *Softwarerepositorys* einsehen (Button *GPG-Keys* unten rechts). Die Fingerabdrücke des seit 2024 eingesetzten Schlüssels für die Standard-Repositories und des Schlüssels für das Packman-Repository mit unbeschnittenen Multimedia-Codecs können Sie aus dem Netz herunterladen. Auch allen Build-Service-Repositories ist ein eigener GPG-Schlüssel zugeordnet, beim Hinzufügen eines neuen Repos erscheint die Abfrage aus Abbildung 3. Auf der Webseite des Build-Service finden Sie den Fingerprint nach einem Klick auf den blauen Link zum OBS-Projekt ganz oben links unter *Home* im Reiter *Signing Keys* 4.

Das von Suse genutzte Paketsystem RPM gestattet es zu prüfen, ob sich in den Paketen enthaltene Dateien seit der Installation verändert haben. Das wäre etwa der Fall, hätte ein Virus eine Programmdatei infiziert. Das Kommando aus der ersten Zeile von Listing 1 liefert eine Liste von Dateien, die sich vom Inhalt des Pakets unterscheiden. Bei vielen davon sind allerdings Veränderungen zu erwarten, und sie stellen keinen Hinweis auf eine Manipulation dar.

Der Befehl aus der zweiten Zeile von Listing 1 siebt durch den ersten Grep-Aufruf alle Konfigurations- und Ghost-Dateien aus. Bei letzteren handelt es sich um zur Laufzeit entstehende Dateien, die die Installation nicht einspielt, die ein Entfernen des Pakets aber löscht. Die zweite Grep-Stufe filtert aus den dann noch verbleibenden schließlich alle Dateien heraus, deren Dateigröße (S), Inhalt (5) oder Erstellungszeit (T) sich nachträglich verändert hat.



1 Heutzutage geben die für die Internetverbindungen zuständigen Router wie die hier zu sehende Fritz!Box standardmäßig keinerlei Ports frei. Alle angeschlossenen Rechner sind damit gegen von außen initiierte Verbindungen vollständig abgeschottet.

Listing 1: Pakete prüfen

```
$ rpm -Va
$ sudo rpm -Va | grep -Ev " c |
g " | grep -E "S\.|\.5|\.T"
$ rpm -Qf /Pfad/GeänderteDatei
```

Dezentral

Ob die inzwischen verbreiteten distributionsübergreifenden Flatpak-Pakete ebenso sicher sind wie die von den Distributionen mitgelieferten Pakete, ist Gegenstand anhaltender Diskussionen. Flatpaks beziehen zwar verbreitete Abhängigkeiten wie die Gnome- oder KDE-Komponenten aus gut gepflegten Laufzeitumgebungen, jedes Flatpak

Listing 2: Flatpaks nutzen

```
$ flatpak remote-add --if-not-exists flathub https://flathub.org/repo/
flathub.flatpakrepo
$ gpg --show-keys --with-fingerprint /var/lib/flatpak/repo/flathub.
trustedkeys.gpg
$ flatpak remote-add --if-not-exists --subset=verified flathub-verified
https://flathub.org/repo/flathub.flatpakrepo
```

Listing 3: override.conf

```
[Mount]
Options=noexec
```

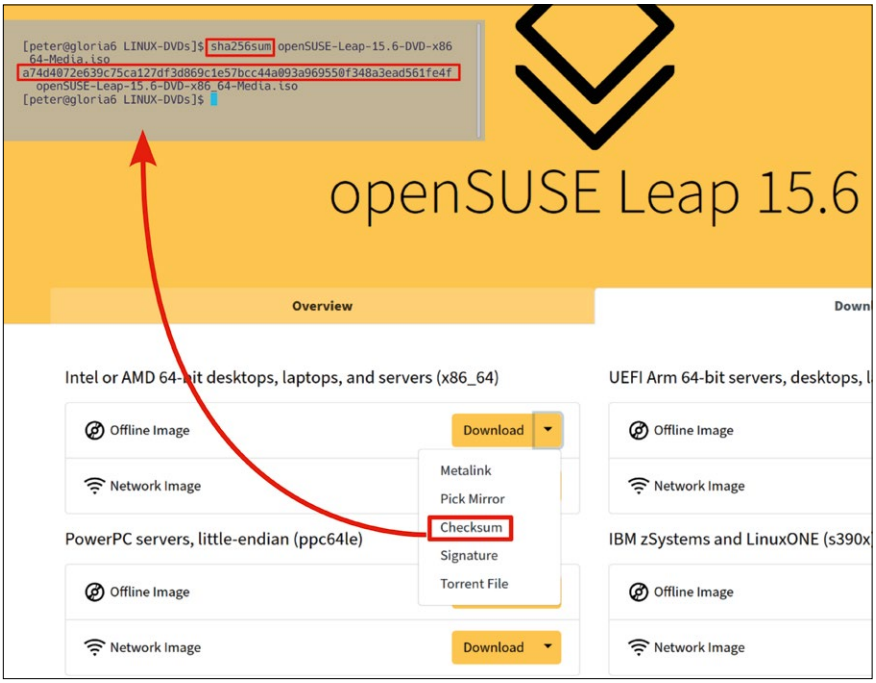
bringt aber eben auch alle seine spezifischen Abhängigkeiten separat mit.

Das lässt Erinnerungen an das als „DLL hell" bekannte Bibliothekschaos unter Windows aufkommen. Windows-Programme liefern mangels eines zentralen Versionsmanagements traditionell eigene Versionen von Bibliotheken mit, die dann parallel in verschiedenen Fassungen auf dem System vorliegen und bei Sicherheitslücken schwer zuverlässig auszutauschen sind.

Entsteht eine Sicherheitslücke in einer nicht von den Laufzeitumgebungen abgedeckten Bibliothek, muss jeder einzelne Flatpak-Autor aktiv das in seinem Paket genutzte Hilfsprogramm aktualisieren. Bei vielen auf dem Rechner installierten Flatpaks steigt damit die Wahrscheinlichkeit an, dass eine ungepatchte Version auf dem System verbleibt.

Als Sicherheitsplus gilt die Kapselung von Flatpak auf Basis des Containersystems Bubblewarp. Doch das Unterbinden des Dateizugriffs auf das System außerhalb des Containers ist eher eine theoretisch bestehende technische Möglichkeit als eine flächendeckend zum Zuge kommende Praxis 5. Denn die Anwender erwarten schlicht, dass sie die Daten eines Programms an einer beliebigen Stelle im Home-Verzeichnis speichern können. Darum gewähren ihnen die Flatpak-Autoren per Paketeinstellungen großzügig diesen Schreibzugriff auf das gesamte Benutzerverzeichnis.

Wer Pakete auf Flathub.org veröffentlichen will, dem Standard-Repository für Flatpaks, muss einen Antrag stellen. Der, so schreiben die Betreiber, zieht eine Überprüfung der Pakete nach sich. Zusätzlich finden laufend automatisierte Scans nach Sicherheitsproblemen statt. Dennoch dürfte es weitaus schwieriger sein, verdächtige Aktivitäten unter Tausenden Paket-Maintainern auszumachen als in einem Distri-Team mit vielleicht zweistelliger Mitgliederzahl.



2 Echtheitskontrolle vor der Installation: Der Aufruf von Sha256sum muss für das heruntergeladene ISO-Image dieselbe Zeichenfolge liefern wie die nach einem Klick auf den Pfeil des Download-Buttons erscheinende Seite *Checksum*.

Zugriffe regeln

Sie können die Flatpak-Sicherheit durch ein Beschränken der Berechtigungen selbst erhöhen. KDE-Anwender brauchen dazu nur das Modul *Flatpak-Berechtigungen* in der KDE-Systemsteuerung zu öffnen. Anwender anderer Desktop-Umgebungen installieren dafür das Programm Flatseal vom OpenSuse Build Service. Die Version des Build-Service-Benutzers *Dead_Mozay* hat im Test einwandfrei funktioniert. Zur Gegenkontrolle nennt die Paketverwaltung den Fingerprint des GPG-Schlüssels zum Repository beim Hinzufügen der Quelle.

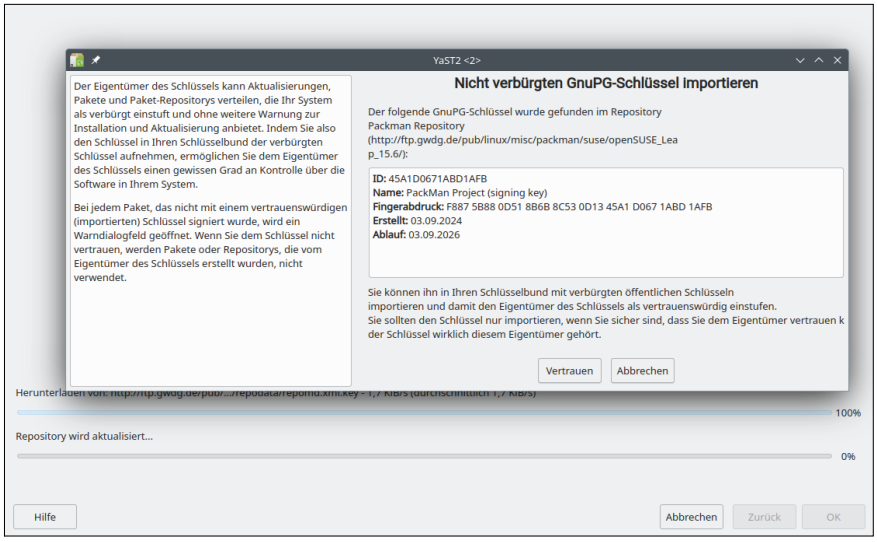
Flatseal und auch die KDE-Systemsteuerung erlauben es unter anderem, Programmen einen im Flatpak-Paket eigentlich vorgesehenen Schreibzugriff für das gesamte `/home` nachträglich zu entziehen und die Freigabe auf bestimmte Ordner einzuschränken.

Flathub signiert alle Pakete mit einem gemeinsamen Schlüssel und sichert genau wie das Suse-Paketsystem die Dateiübertragung per Internet. Der Anwender bekommt den Schlüssel allerdings nie zur Prüfung zu Gesicht, es sei denn, er ruft per Hand nach Aktivieren des Flathub-Repositorys (Listing 2, erste Zeile) ein entsprechendes Kommando auf (zweite Zeile). Der Referenzschlüssel lässt sich im Browser herunterladen und ebenfalls per `gpg --show-keys` auf seinen Fingerprint prüfen.

Zur Gewährleistung der Sicherheit müssen Sie Flatpaks genau wie gewöhn-

liche Pakete immer aktuell halten. Für OpenSuse-Packages signalisiert ein Taskleisten-Icon das Bereitstehen von Updates, bei Flatpaks ist das unter Suse nicht der Fall: Die grafischen Software-management-Apps KDE Discover und Gnome Software unterstützen Flatpak, nicht jedoch die Suse-Softwareverwaltung. Am einfachsten lassen sich daher die installierten Flatpaks inklusive der Runtimes per Eingabe von `sudo flatpak update` aktuell halten.

Wie erwähnt, steht die Publikation eigener Pakete auf Flathub allen frei. Bei mit einem blauen Häkchen als verifiziert ausgewiesenen Paket 6 hat die Überprüfung ergeben, dass es sich beim Veröffentlicher um den eigentlichen Entwickler der Software handelt. Projekte und Firmen veröffentlichen immer häufiger ein für alle Linux-Distributionen verwendbares Flatpak. So können Sie ihre Software unabhängig von den Aktualisierungszyklen der Distributionen in einer aktuellen Version verteilen. Möchten Sie auf ihrem System nur verifizierte Flatpaks installieren, erreichen Sie das mit dem Kommando aus der letzten Zeile von Listing 3. Nur Suchtreffer aus dem geprüften Repository *flathub-verified* erfüllen die darin gestellte Bedingung.

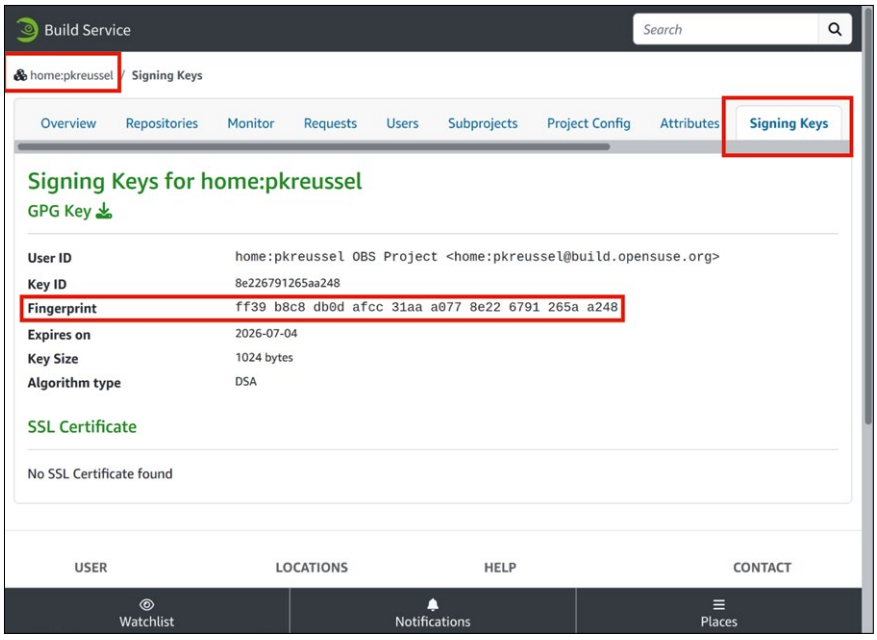


3 Beim Hinzufügen eines neuen Repositorys fragt YaST, ob es dem noch unbekannten GnuPG-Schlüssel vertrauen soll. Sie sollten dem nur zustimmen, wenn Sie sich sicher sind, dass *der Schlüssel wirklich diesem Eigentümer gehört***.**

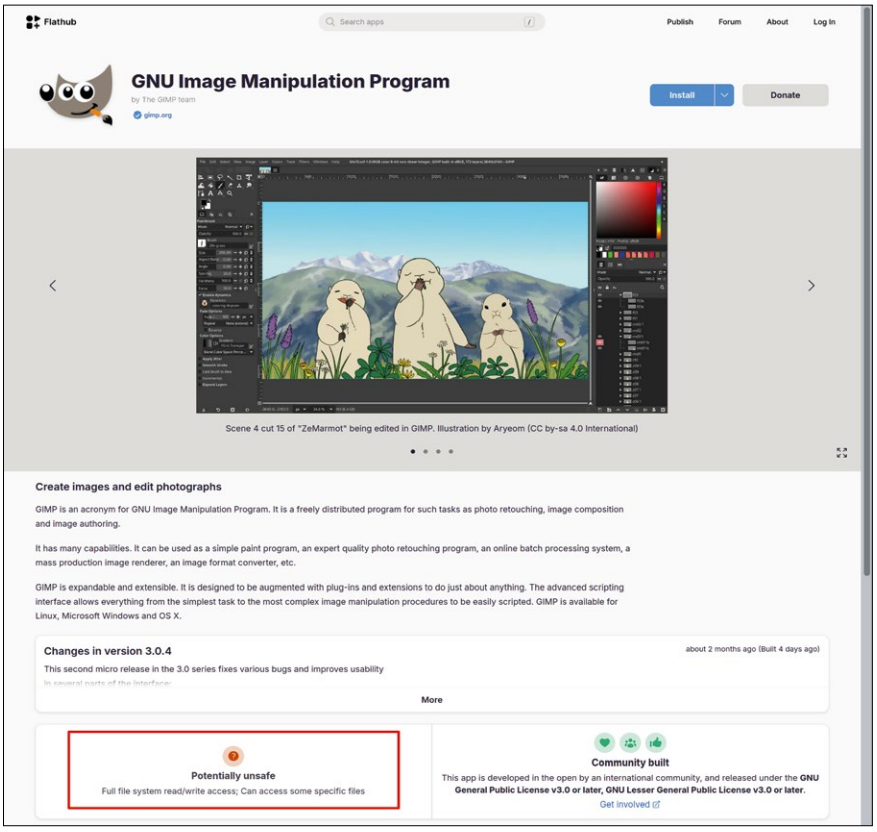
Eingehegt

Bei per Flatpak installierter Software handelt es sich meist um Programme wie Bitmap-Editoren oder Textverarbeitungen, die Angriffen aus dem Internet weniger ausgesetzt sind als ein Webbrowser. Doch das kann sich schnell ändern, sobald Sie damit Dateien aus einer unbekannten Quelle öffnen: Bei Anwendungen mit Fehlern in der Speicherverwaltung (die sich manchmal in Abstürzen äußern) ist es potenziell möglich, durch präparierte Dateien eigenen Code mit Benutzerrechten auszuführen.

Einem Angreifer bliebe es so zwar verwehrt, Systemdateien zu verändern oder bösartigen Code in den Kernel einzuschleusen. Doch es ist für Schadsoftware dennoch ein Leichtes, bei jedem Anmelden startende Skripte in den dafür vorgesehenen Verzeichnissen zu installieren. Diese Skripte loggen dann selbst ohne Root-Zugriff unter X11 alle Tastatureingaben mit. Bei Wayland-Programmen funktioniert dieses Vorgehen nicht so leicht. Im Verzeichnis `~/.config/autostart/` finden sich die Starter für bei jedem Login aufgerufene Programme. KDE führt außerdem vor jedem Login noch Skripte unter `~/.config/plasma-workspace/env/` aus, zum Beispiel, um Umgebungsvariablen zu setzen.



4 Für jedes Projekt auf dem OpenSuse-Build-Service, sei es das Home-Projekt eines externen Accounts oder ein offizielles OpenSuse-Projekt, gibt es einen eigenen Schlüssel für die Signatur der dort erstellten Repositories.



5 Die meisten Flatpaks auf Flathub sind potenziell unsicher und für vollen Lese- und Schreibzugriff auf das Dateisystem des Rechners konfiguriert.

Listing 4: Firejail

```
$ sudo zypper in firejail
$ sudo usermod –a –G firejail Benutzer
```

Wasm: Webassembly. Offener Standard des W3C für portablen Bytecode zum Ausführen von Programmen innerhalb eines Webbrowsers.

Zum Glück gibt es einige Schutzmaßnahmen, um Schadsoftware auf Benutzerebene das Leben schwerer zu machen: Die Mount-Option `noexec` weist den Linux-Kernel an, aus einer damit eingehängten Partition keinen Programmcode auszuführen. Es ist deshalb generell keine schlechte Idee, die Home-Partition auf diese Weise zu mounten. Das System bringt ausführbare Dateien nicht ohne Grund vor Schreibzugriffen mit Benutzerrechten geschützt in eigenen Verzeichnissen unter. Das Standard-Partitionslayout von OpenSuse listet auch `/var` als separates Btrfs-Volume, das sich mit Ausführsperre einhängen lässt.

Um Ihr Home-Verzeichnis auf diese Weise zu schützen, fügen Sie der entsprechenden Zeile in `/etc/fstab` einfach die `noexec`-Option hinzu 7. Dabei darf dann weder vor noch nach dem Komma hinter `home` ein Leerzeichen stehen, sonst startet der Rechner nicht mehr. Unter OpenSuse Leap 15.6 lässt sich auch `/tmp` auf diese Weise in Fstab modifizieren, ein Verzeichnis, in das jeder Anwender schreiben darf. Tumbleweed erzeugt unter Systemd das `/tmp`-Verzeichnis dagegen dynamisch. Hier legen Sie dann stattdessen die Datei `/etc/systemd/system/tmp.mount.d/override.conf` mit dem Inhalt aus Listing 3 an.

Die `noexec`-Option verhindert zudem den direkten Start von Shell-Skripten, zum Beispiel mit einem Klick im Dateimanager. Sie lassen sich dann nur noch in der Shell via `sh /Pfad/zum/Skript.sh` ausführen. Da es sich bei den Desktop-Dateien der Autostart-Einträge in `~/.config/autostart/` nicht um ausführbare Dateien handelt, funktionieren sie trotz `noexec` weiter. Nichts hindert also einen Angreifer daran, Schreibzugriffe auf das Home dort in einem Shell-Skript abzulegen und es bequem per Autostart-Eintrag zu starten.

Die Ausführungsprävention mit `noexec` verhindert also das Starten von gewöhnlichen ausführbaren Dateien aus dem Home, jedoch nicht den Aufruf von Shell-Skripten. Sie sind dann in der Lage, Dateien im Home zu löschen oder mit den auf den meisten Systemen installierten Tools zu verschlüsseln.

Autostart-Skripte, die Schadsoftware bei jedem Anmelden am System aktivieren, lassen sich relativ leicht entdecken. Das gilt jedoch nicht für Bedrohungen, denen der Webbrowser ausgesetzt ist. Er steht direkt mit dem Internet in Kontakt, ist komplex und stellt in Form von Javascript und Wasm sogar Programmiersprachen bereit.

Eine im Browser eingebaute Sandbox soll das System vor Angriffen bösartiger Webseiten schützen. Doch Bugs, die einen Ausbruch aus dieser Schutzhülle gestatten („Sandbox Escape“) gab es schon häufiger. Vorsichtige Anwender umgeben den Browser mithilfe des einfach zu benutzenden Tools Firejail mit einem zusätzlichen Schutzcontainer. Das funktioniert prinzipiell bei jedem Programm. Es genügt dafür, dem Aufruf auf der Konsole `firejail` voranzustellen, zum Beispiel `firejail firefox`.

Das Werkzeug Firejail richten Sie mit den Kommandos aus Listing 4 ein und starten dann das System neu. Das Tool bringt Profile für eine ganze Reihe gängiger Programme mit. Im Fall von Firefox gestattet es den Schreibzugriff auf das Profilverzeichnis unter `~/.mozilla/fire-`

`fox`, ohne den der Browser nicht funktioniert. Überdies darf der Anwender heruntergeladene Dateien im Verzeichnis `~/Downloads` ablegen.

Brandmauer

Die bildhafte Bezeichnung Firewall suggeriert dem Nutzer maximale Sicherheit hinter einer schützenden Wand, obwohl sie unter Linux-Systemen eher ein Behelfspflaster für Lücken darstellt, die es gar nicht geben müsste.

Das Eindringen in fremde Computer von außen gelingt nur über Serverdienste, die entweder Befehle ausführen, ohne die Berechtigungen zu prüfen, oder die aufgrund von Speicherlücken das Einschleusen von fremdem Code ermöglichen. Netzwerkdienste, die von vornherein nicht laufen, sind in Sachen Sicherheit per Firewall abgeschirmten unsicheren Diensten vorzuziehen. Wenn Sie kein Remote-Login nutzen, deaktivieren Sie den zugehörigen SSH-Dienst mit dem Befehl aus der ersten Zeile von Listing 5. Das Kommando aus der zweiten Zeile aktiviert ihn bei Bedarf wieder.

OpenSuse verfährt dennoch seit Jahren nach der Devise, dass eine zusätzliche Schutzschicht nicht schadet, und aktiviert die Firewall standardmäßig. Schon bei der Installation dürfen Sie hier aber den Port für SSH und den Remote-Login-Dienst schließen 8, den SSH-Dienst deaktivieren oder die Firewall ganz ausschalten. Ist der entsprechende Port in der System-Firewall und im Internet-Router freigegeben, lässt sich der Rechner auch aus dem Internet erreichen, wie es sich viele Anwender wünschen.

In der Standardkonfiguration hält nur ein Passwort Eindringlinge fern, die zahlreich und automatisiert an erreichbare SSH-Ports anklopfen. Das Kommando `sudo journalctl –u sshd –g "Failed password"` fördert die zugehörigen Einträge im Systemjournal zutage. Ist das Passwort sicher, besteht also nicht aus in Wörterbüchern zu findenden Bestandteilen, kommen Angreifer nicht weit.

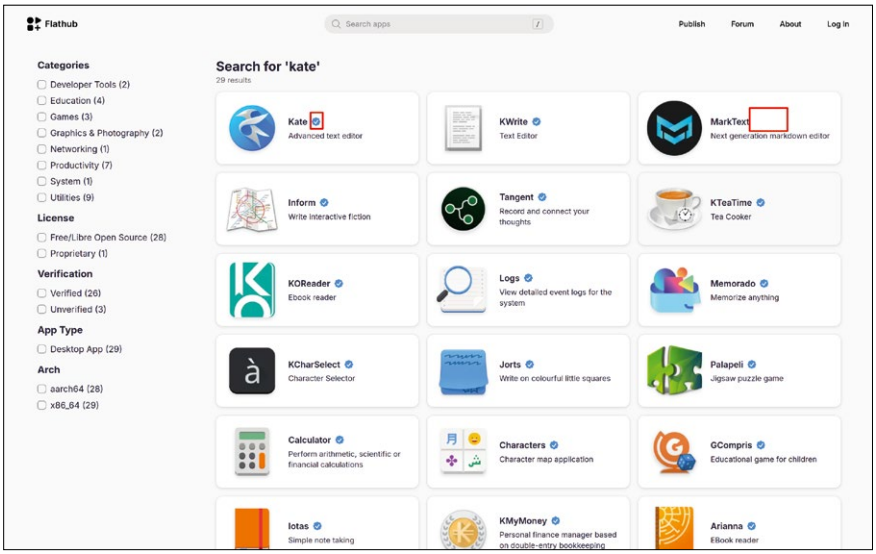
Dennoch stellen Sie den Zugang von außen besser per VPN her und halten alle Ports in der Router-Firewall geschlossen. Zudem empfiehlt es sich, SSH auf schlüsselbasierte Authentifikation umzustellen. Ein Passwort genügt dann nicht mehr für das Login. Nur wer eine passende Schlüsseldatei vorzeigt, deren Länge Zufallstreffer ausschließt, darf passieren. Solche Schlüsseldateien lassen sich noch zusätzlich durch ein Passwort sichern, sodass Angreifern der Besitz des Schlüssels allein nicht genügt.

Erstellen Sie zuerst einen SSH-Schlüssel auf einem der Rechner, von dem aus Sie sich aus dem Internet einloggen möchten (der Client), während er sich im Heimnetz befindet. Das Ausführen von `ssh–keygen` genügt dafür. SSH fordert Sie dabei zum Bestätigen des Schlüsseldateinamens und -pfads und zur zweimaligen Eingabe eines Passworts auf. Kopieren Sie den soeben generierten Schlüssel mittels Eingabe des Befehls `ssh–copy–id` *`IP–Adresse`* auf den Rechner, auf den Sie sich remote einloggen möchten (Server). Die aus vier dreistelligen Zahlen bestehende IPv4-Adresse im Heimnetz finden Sie per `ip a` auf dem Zielrechner heraus. Ein Login per SSH auf diesen Computer muss dabei möglich sein, sprich: Der SSH-Dienst muss dort laufen und der Firewall-Port offen sein.

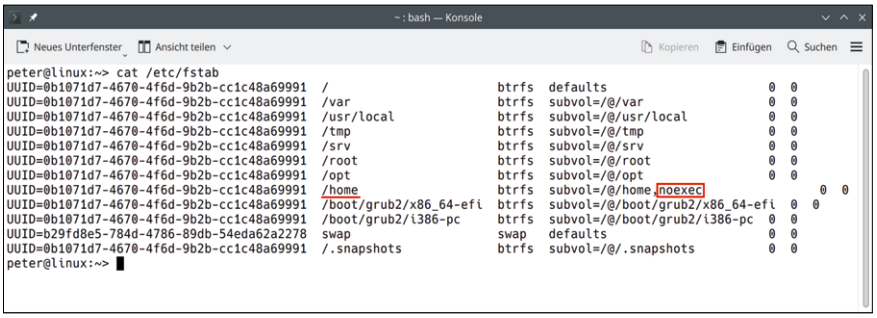
Testen Sie das Login von dem Rechner aus, zu dem Sie den Schlüssel übertragen haben. Das Kommando `ssh` *`IP–Adresse`* sollte mit der Aufforderung `Enter passphrase for key ...` antworten. Das Schlüsselwort `key weist` darauf hin, dass ein Schlüssel zur Authentifizierung zum Einsatz kommt.

Listing 5: SSH deaktivieren

```
$ sudo systemctl disable sshd --now
$ sudo systemctl enable sshd --now
```



6 Viele Pakete auf Flathub tragen inzwischen den Verified-Haken, der besagt, dass die Entwickler der Software selbst das Flatpak erstellt haben.



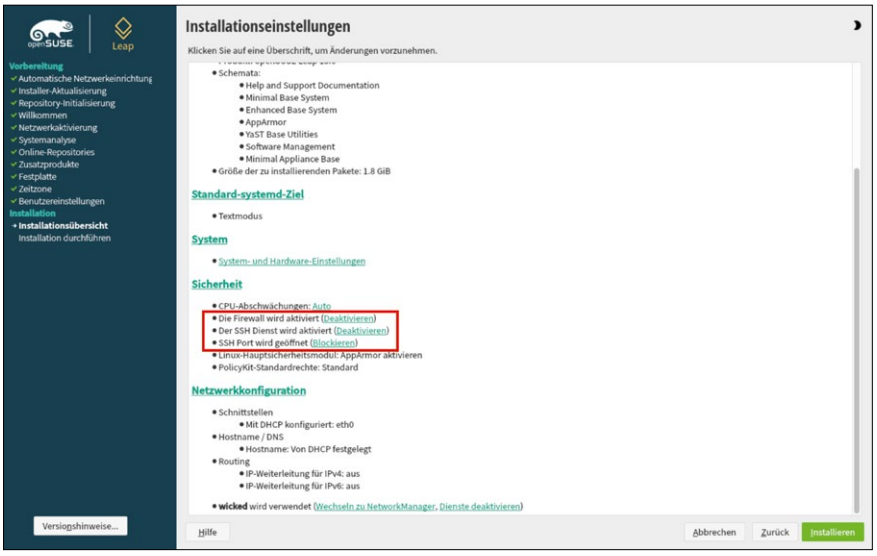
7 Das simple Hinzufügen der Option `noexec` in der für das Home-Verzeichnis zuständigen Zeile der `/etc/fstab` unterdrückt das Starten von im Home abgelegten Binaries.

Listing 6: Authentifizierung einschränken

```
PasswordAuthentication no
AuthenticationMethods publickey
```

Noch ist das schlüsselbasierte Login aber nicht die einzige Möglichkeit zur Anmeldung. Drücken Sie die Eingabetaste, statt das Schlüsselpasswort zu tippen, dann erscheint im jetzigen Zustand die Aufforderung, das Benutzerpasswort einzugeben. Das ändert sich, nachdem Sie als Root auf dem Server im Verzeichnis `/etc/ssh/sshd_config.d/` die Datei `20-force_publickey_auth.conf` mit dem Inhalt aus Listing 6 angelegt haben.

Um die Konfigurationsänderung scharfzuschalten, starten Sie den SSH-Daemon mit `sudo systemctl restart sshd` neu. Danach sollte beim SSH-Login mit `ssh` *`IP-Adresse`* nach Drücken der Eingabetaste ohne Passworteingabe nicht länger eine zweite Aufforderung erscheinen, sondern die Meldung `Permission denied (publickey)`. Das SSH-Login ist nun gegen Brute-Force-Attacken per Durchprobieren des Passworts geschützt. Das Einloggen klappt nur noch von Rechnern aus, deren Login-Schlüssel Sie mit `ssh-copy-id` auf den Server übertragen haben.



8 Voreinstellungen bei der OpenSuse-Installation für Firewall und Remote-Login per SSH: Die Firewall ist mit geöffnetem SSH-Port aktiv, der Remote-Login-Dienst läuft.

Ausblick

Ein jüngeres Beispiel für eine über offizielle Distributionspakete ausgelieferte Bedrohung war die äußerst kritische Backdoor in der Kompressionsbibliothek Xz Anfang 2024. Der SSH-Server lud diese Bibliothek auch unter Tumbleweed über einen nicht nur von Suse eingesetzten Patch und verschaffte so einem Eindringling ohne Authentifizierung Root-Rechte. Wäre diese Backdoor per Paket-Upgrade in großer Anzahl auf Produktivsysteme mit Debian Stable oder SLES gelangt, hätte dort ein Scheunentor für Angriffe offengestanden.

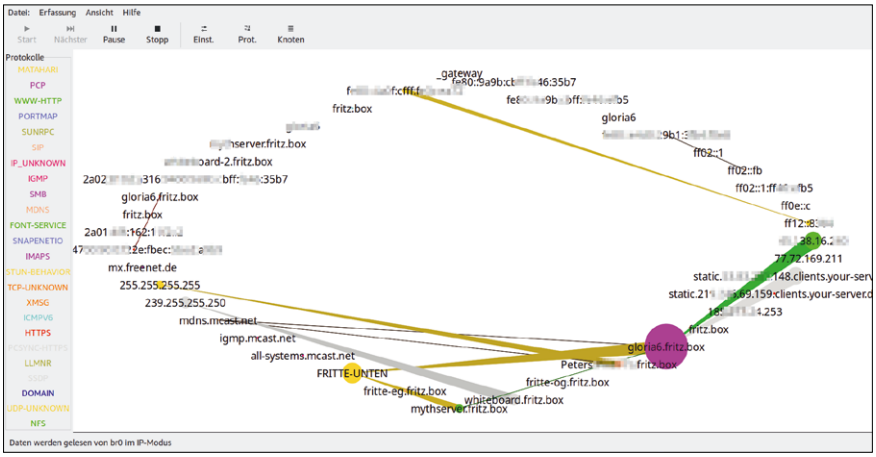
Dass das nicht in großem Stil passierte, ist der Aufmerksamkeit des PostgreSQL- und Microsoft-Entwicklers Andres Freund zu verdanken. Er wollte sich nicht damit abfinden, dass auf seinem Debian Unstable nach einem Update beim Einloggen per SSH plötzlich eine ungewöhnlich hohe CPU-Last auftrat. Letztlich wendeten er und die schnelle Reaktion der Linux-Distributionen großen Schaden gerade noch ab.

Zwei Dinge lassen sich daraus ableiten: Wer sein System kennt, entwickelt ein Gefühl dafür, wenn es sich plötzlich unerwartet verhält. Kommandozeilenwerkzeuge wie Top und Htop oder der unter KDE mit [AltGr]+[Esc] zu öffnende grafische Systemmonitor informieren jederzeit über die CPU-Last sowie die Speicherbelegung und zeigen, wie sie sich auf einzelne Prozesse mit bestimmten Namen verteilen. Im Internet tauchen in Foren oft Fragen bezüglich des hohen Speicherverbrauchs oder der exzessiven CPU-Last bestimmter Prozesse auf. Solche Fragen zu stellen, ist richtig, auch wenn ein Bug immer noch die wahrscheinlichere Erklärung dafür ist als ein böswilliger Angriff auf den Rechner.

Wichtig sind für Suse-Anwender das Tool Zypper-log beziehungsweise der Menüpunkt *Extras/Verlauf anzeigen* im YaST-Modul *Software*. Beide zeigen eine Dokumentation aller Aktionen des Paket-

managements wie Installationen und Upgrades, die Auslöser eines veränderten Verhaltens sein könnten.

Auch der grafische Netzwerkmonitor Etherape 9, der den Netzwerkdatenverkehr im Heimnetz und im Internet je nach übertragener Datenmenge als unterschiedlich dicke Balken darstellt, empfiehlt sich für Benutzer als diagnostisches Werkzeug. Das Monitoring-Werkzeug macht so verdächtige Datenströme direkt sichtbar, ohne dass der Anwender sich in die Interna der Netzwerkprotokolle einarbeiten muss. (*uba/jlu*)



9 Etherape visualisiert, zwischen welchen Rechnern im lokalen Netz und welchen Internetadressen Daten fließen. Die Dicke der Linien zeigt die Übertragungsgeschwindigkeit.

Weitere Infos und interessante Links

www.linux-user.de/qr/52021#

COMPUTEC
marquard group

Ein Unternehmen der MARQUARD MEDIA GROUP AG
Verleger: Jürg Marquard

Redaktion/Verlag	Computec Media GmbH Redaktion LinuxUser Dr. -Mack-Straße 83 90762 Fürth Telefon: (0911) 2872-110 E-Mail: redaktion@linux-user.de Web: www.linux-user.de
Geschäftsführer	Rainer Rosenbusch
Chefredakteur, Brand/Editorial Director	Jörg Luther (jlu, v. i. S. d. P.), joerg.luther@computec.de
Stellv. Chefredakteurin Strategy & Operations	Carina Schipper (csi), carina.schipper@computec.de
Redaktion	Uli Bantle (uba), ulrich.bantle@computec.de Thomas Leichtenstern (tle), thomas.leichtenstern@computec.de
Linux-Community	Jörg Luther, joerg.luther@computec.de
Datenträger	Thomas Leichtenstern (tle), cdredaktion@linux-user.de
Ständige Mitarbeiter	Erik Bärwaldt, Hans-Georg Eßer, Peter Kreußel, Claudia Meindl, Thomas Reuß, Tim Schürmann (tsc), Anna Simon, Daniel Tibi, Ferdinand Thommes, Uwe Vollbracht, David Wolski (dwo)
Titel & Layout	Titel: Alexandra Böhm Titelmotiv: Maksym Yemelyanov Layout: Alexandra Böhm
Sprachlektorat	Stefan Gneiting, Sabine Schmitt
Produktion	Martin Closmann (Ltg.), martin.closmann@computec.de Uwe Hönig, uwe.hoenig@computec.de
Anzeigen	Verantwortlich für den Anzeigenteil: Bernhard Nusser Es gilt die Anzeigenpreisliste vom 01.01.2024.
Mediaberatung D/A/CH	Bernhard Nusser, bernhard.nusser@computec.de Tel.: (0911) 2872-254, Fax: (0911) 2872-241
Mediaberatung UK/USA	Brian Osborn, bosborn@linuxnewmedia.com
New Business	Viktor Eippert (Project Manager)
E-Commerce & Affiliate	Daniel Waadt (Head of E-Commerce & Affiliate), Veronika Maucher, Andreas Szedlak, Frank Stöwer
Abo	Die Abwicklung (Rechnungsstellung, Zahlungsabwicklung und Versand) erfolgt über unser Partnerunternehmen: DPV Deutscher Pressevertrieb GmbH Leserservice Computec 20080 Hamburg Deutschland
Einzelhefte und Abo-Bestellung	https://shop.computec.de
Leserservice Deutschland	Ihre Ansprechpartner für Reklamationen und Ersatzbestellungen E-Mail: computec@dpv.de Tel.: (0911) 99 39 90 98 Fax: (01805) 861 80 02* (* 0,14 €/min via Festnetz, max. 0,42 €/min via Mobilnetz)
Österreich, Schweiz	E-Mail: computec@dpv.de
und weitere Länder	Tel.: +49 911 99399098 Fax: +49 1805 8618002
Supportzeiten	Montag 07:00 – 20:00 Uhr, Dienstag – Freitag: 07:30 – 20:00 Uhr, Samstag 09:00 – 14:00 Uhr
Pressevertrieb	DMV Der Medienvertrieb GmbH & Co. KG Meßberg 1, 20086 Hamburg http://www.dermedienvertrieb.de
Druck	EDS Zrínyi Zrt., Nádas utca 8, 2600 Vác, Ungarn
ISSN	1615-4444

marquard group

Deutschland:

4PLAYERS, AREAMOBILE, BUFFED, GAMESWORLD, GAMESZONE, GOLEM, LINUX-COMMUNITY, LINUX-MAGAZIN, LINUXUSER, N-ZONE, GAMES AKTUELL, PC GAMES, PC GAMES HARDWARE, PC GAMES MMORE, PLAY 4, RASPBERRY PI GEEK, VIDEOGAMESZONE

Marquard Media Hungary:

JOY, JOY-NAPOK, INSTYLE, SHOPPIEGO, APA, ÉVA, GYEREKLÉLEK, FAMIILY.HU, RUNNER`S WORLD

ABONNEMENT

Probeabo (3 Ausgaben)	Deutschland	Österreich	Schweiz
No-Media-Ausgabe	15,00 €	15,00 €	15,00 €
DVD-Ausgabe	19,00 €	19,00 €	19,00 €
Jahres-Abo (12 Ausgaben)	**Deutschland**	**Österreich**	**Schweiz**
No-Media-Ausgabe	91,00 €	99,00 €	106,00 €
DVD-Ausgabe	112,00 €	120,00 €	127,00 €
Jahres-DVD zum Abo *	6,70 €	6,70 €	6,70 €
Preise Digital	**Deutschland**	**Österreich**	**Schweiz**
Heft-PDF Einzelausgaben Digital	8,50 €	8,50 €	8,50 €
Digital-Abo (12 Ausgaben)	84,99 €	84,99 €	84,99 €
Kombi Digital + Print (No-Media-Ausgabe, 12 Ausgaben)	103,00 €	111,00 €	118,00 €
Kombi Digital + Print (DVD-Ausgabe, 12 Ausgaben)	124,00 €	132,00 €	139,00 €

Die Probe-, Jahres- und Digital-Abos erhalten Sie in unserem Webshop unter https://shop.computec.de. Die Auslieferung erfolgt versandkostenfrei.

(*) Nur erhältlich in Verbindung mit einem Jahresabonnement der Printausgabe von LinuxUser.

Internet	https://www.linux-user.de
News und Archiv	https://www.linux-community.de
Facebook	https://www.facebook.com/linuxuser.de

Schüler- und Studentenermäßigung: 20 Prozent gegen Vorlage eines Schülerausweises oder einer aktuellen Immatrikulationsbescheinigung. Der aktuelle Nachweis ist bei Verlängerung neu zu erbringen. Andere Abo-Formen, Ermäßigungen im Ausland etc. auf Anfrage. Adressänderungen bitte umgehend beim Kundenservice mitteilen, da Nachsendeaufträge bei der Post nicht für Zeitschriften gelten.

Rechtliche Informationen

LinuxUser Community Edition

LinuxUser gibt es auch als Community-Edition: Dabei handelt es sich um eine rund 30-seitige PDF-Datei mit ausgewählten Artikeln aus der aktuellen Ausgabe, die parallel zur Veröffentlichung des gedruckten Hefts erscheint.

Die kostenlose Community-Edition steht unter einer Creative-Commons-Lizenz, die es erlaubt, „das Werk zu vervielfältigen, zu verbreiten und öffentlich zugänglich machen". Sie dürfen die LinuxUser Community-Edition also beliebig kopieren, gedruckt oder als Datei an Freunde und Bekannte weitergeben, auf Ihre Website stellen – oder was immer Ihnen sonst dazu einfällt. Lediglich bearbeiten, verändern oder kommerziell nutzen dürfen Sie sie nicht. Darum bitten wir Sie im Sinn des „fair use". Weitere Informationen finden Sie unter: http://linux-user.de/CE

Probleme mit den Datenträgern

Falls es bei der Nutzung der Heft-DVDs zu Problemen kommt, die auf einen defekten Datenträger schließen lassen, dann schicken Sie bitte eine E-Mail mit einer genauen Fehlerbeschreibung an die Adresse computec@dpv.de. Wir senden Ihnen dann umgehend kostenfrei einen Ersatzdatenträger zu.

README

In jedem Artikel in diesem Heft liefern spezielle Auszeichnungen und grafische Elemente wichtige Zusatzinformationen zum Text.

Der Mensch lebt nicht vom Text allein: Zu jedem Artikel in diesem Heft gehören eine Reihe von Zusatzinformationen, die das bloße Narrativ um weiterführende Inhalte ergänzen. Manche davon integrieren sich direkt in den Textfluss, andere stehen als gesonderte grafische Elemente in der sogenannten Marginalspalte, also dem teilweise freien Bereich an der rechten beziehungsweise linken Seitenkante.

Typografische Konventionen

Eine blaue Einfärbung hebt Verweise auf Tabellen und Kästen hervor: siehe Kasten *Kastentitel*. Die Kursivierung signalisiert hier wie in vielen anderen Fällen eine symbolische Bezeichnung; in einem Codebrocken könnte das etwa so aussehen:

```
$ cat "EinLängererTextbrocken" >> ⮐
Ausgabe.txt
```

Der „Umbruchhaken“ am Ende der ersten Zeile des Codes verweist hier darauf, dass es sich in diesem Fall eigentlich um eine einzige Eingabezeile handelt, die nur aus Platzgründen im Druck umgebrochen werden musste.

Die Kursivierung kann neben Platzhaltern auch andere Elemente bezeichnen, wie Paketnamen und Benutzerkonten, beispielsweise *build-essential* und *root*. Aber auch Menüpunkte drucken wir kursiv ab, wobei in Menüfolgen eine Pipe die einzelnen Elemente trennt: *Sonstiges* | *Textkodierung* | *Unicode*.

Dateien zum Artikel herunterladen unter

www.linux-user.de/dl/52015

Gelegentlich begegnen Ihnen in den Artikeln auch orangefarbig hinterlegte Textstellen. Sie verweisen auf ein Glossar, das den markierten Begriff kurz erläutert. Sie finden den Glossartext dann in einer der Marginalspalten.

Tasten und Tastenfolgen

Ein Buchstabe oder eine Buchstabenfolge in eckigen Klammern, wie [Esc], steht symbolisch für einen Tastendruck. Dabei dient als Schreibweise grundsätzlich die Beschriftung der Tasten einer deutschen Tastatur. Ein Druck auf [T] erzeugt also ein kleines „t“, die Kombination [Umschalt]+[T] ein großes „T“.

Dabei signalisiert das Pluszeichen zwischen Tasten, dass man sie gleichzeitig drücken muss, ein Komma dagegen, dass sie nacheinander betätigt werden müssen. Das allseits beliebte Copy & Paste gelingt also mit [Strg]+[C], [Strg]+[V].

Lesen Sie etwas von der Super-Taste, handelt es sich dabei um die eigentlich korrekte Bezeichnung der Taste, die in Microsoft-Umgebungen „Windows-Taste“ heißt und auf der bei vielen Tastaturen das entsprechende Logo prangt.

Infos und Downloads

An einzelnen Stellen im Text finden Sie das Zeichen , das auf eine weiterführende Information verweist. Um an die Links zum Artikel zu gelangen, blättern Sie ans Ende des Artikels, wo Sie einen Kasten Weitere Infos und interessante Links finden. Entweder tippen Sie die dort angegebene URL `www.linux-user.de/qr/Nummer` in einen Webbrowser ein – das führt Sie auf eine Webseite mit allen Links zum Artikel –, oder Sie scannen mit dem Smartphone oder Tablet den im Kasten abgedruckten QR-Code ein und surfen so direkt zur Seite mit den Links.

Beispiel für Heft-DVD-Inhalt
`LU/Ordner/`

Glossar: Nähere Definition zum Verständnis eines Begriffs oder einer Abkürzung.

Analog funktioniert der Kasten Dateien zum Artikel herunterladen unter mit der URL `www.linux-user.de/dl/Nummer`. Er bringt Sie auf eine Webseite, die auf interessante Downloads zum Artikel verweist. (Das Exemplar unten links dient nur als Beispiel und führt ins Nirgendwo.)

Heft-DVD

Die preisgünstigere No-Media-Edition von LinuxUser kommt ohne Datenträger, doch die meisten Leser bevorzugen die am Kiosk erhältliche Ausgabe mit Heft-DVD. Bei Artikeln, zu denen Inhalte auf der DVD gehören, finden Sie auf der ersten Doppelseite einen grauen „Halbkreis mit Loch“ (siehe oben), der eine optische Disk symbolisiert. Der Text darunter bezeichnet den zugehörigen DVD-Inhalt und nennt gegebenenfalls auch das Verzeichnis, in dem sich dieser auf dem Datenträger befindet. (*jlu*)

Weitere Infos und interessante Links

www.linux-user.de/52015

Vorschau auf 10/2025

Die nächste Ausgabe erscheint am 19.09.2025

Tools für die Shell

Die Kommandozeile bildet das Herzstück eines jeden Linux-Systems. Selbst eingefleischte Mausschubser räumen ein, dass dort vieles effizienter gelingt als in jeder GUI. Deshalb dreht sich im Schwerpunkt der nächsten Ausgabe alles um die CLI. Wir stellen Ihnen die Neuerungen der taufrischen Bash 5.3 vor und zeigen, mit welchen Werkzeugen Sie in der Shell mathematische Operationen abarbeiten. Außerdem demonstrieren wir, wie Sie mit Cpu-x, Inxi, Hardinfo2 und anderen Tools PC-Hardware auf den Zahn fühlen und wie Sie mit Shfmt ihre Skripte übersichtlich und regelkonform aufbereiten.

Desktop-Verschlüsselung

Nur chiffriert lassen sich persönliche Daten optimal abgesichert in der Cloud, auf Wechseldatenträgern und Massenspeichern ablegen. Wir stellen Ihnen in einem ausführlichen Workshop vier handliche Werkzeuge für die grafische Oberfläche vor, die das Ver- und Entschlüsseln zum Kinderspiel machen.

Paperless-AI

Vor genau einem Jahr haben wir Ihnen das DMS Paperless-NGX zum schnellen Digitalisieren und Archivieren von Dokumenten vorgestellt. Jetzt tritt die Erweiterung Paperless-AI auf den Plan, die über lokale LLMs auf der Basis von Ollama eine automatische Zuordnung und Analyse der Dokumente ermöglicht.

Die Redaktion behält sich vor, Themen zu ändern oder zu streichen.

Heft als DVD-Edition

- 108 Seiten Tests und Workshops zu Soft- und Hardware
- 2 DVDs mit Top-Distributionen sowie der Software zu den Artikeln. Mit bis zu 18 GByte Software das Komplettpaket, das Unmengen an Downloads spart

Heft als No-Media-Edition

- Preisgünstige Heftvariante ohne Datenträger für Leser mit Breitband-Internet-Anschluss
- Artikelumfang identisch mit der DVD-Edition: 108 Seiten Tests und Workshops zu aktueller Soft- und Hardware

Community-Edition-PDF

- Über 30 Seiten ausgewählte Artikel und Inhaltsverzeichnis als PDF-Datei
- Unter CC-Lizenz: Frei kopieren und beliebig weiter verteilen
- Jeden Monat kostenlos per E-Mail oder zum Download

DVD-Edition (10,99 Euro) oder No-Media-Edition (8,99 Euro) Einfach und bequem versandkostenfrei bestellen unter:

http://www.linux-user.de/bestellen

Jederzeit gratis herunterladen unter:

http://www.linux-user.de/CE

Neues auf der Heft-DVD

Die Heft-DVD liegt ausschließlich der LinuxUser DVD-Edition bei.

AxOS 25.06: Einsteigerfreundliches Arch-Linux-Derivat

Das auf Arch Linux basierende AxOS will durch Einführung grafischer Werkzeuge die Systemverwaltung von Arch Linux erleichtern. Außerdem sollen neue, sehr schlanke Arbeitsoberflächen das gesamte System agiler wirken lassen. Die Distribution bringt eine eigene zu Pacman kompatible Paketverwaltung namens Epsilon mit. Sie bedienen sie auf der Kommandozeile mithilfe einer leicht verständlichen Syntax. Sie integriert außer den Arch-Linux-Repositories auch ein AxOS-eigenes. Das Projekt bietet die Distribution in zwei Varianten an: Eine für Rechner mit Nvidia-Grafikkarten und eine für PCs mit AMD/Intel-Chipsatzgrafik. Sie booten beide Varianten live von der DVD, die ISOs finden Sie unter `isos/`. ➥ S. 6

YunoHost 12: Server-Power auf Knopfdruck

Die auf Debian basierende Server-Distribution YunoHost zielt darauf ab, das Selbst-Hosting von Onlinediensten so einfach wie möglich zu gestalten. Die Distribution richtet sich primär an technisch wenig versierte Anwender, die eigene Webanwendungen wie Nextcloud, E-Mail-Dienste, Messenger oder Blogs auf einem eigenen Server betreiben möchten. Gegenüber dem Vorgänger, der auf Debian 11 „Bullseye“ aufbaut, profitiert das aktuelle Release von der Umstellung auf Debian 12 „Bookworm“ als Basis. Die Distribution bietet eine benutzerfreundliche Weboberfläche, über die Sie Anwendungen mit wenigen Klicks installieren, verwalten und aktualisieren. Sie booten YunoHost von der Heft-DVD.

Debian Live Testing „Trixie“: Der Stand der Dinge

Bei Debian Live Testing handelt es sich um eine spezifische dynamische Momentaufnahme der populären Distribution. Sie erlaubt einen Blick auf das nächste Major Release 13 alias „Trixie“. Die finale Fassung erscheint voraussichtlich im ersten Quartal 2026. Außer von den üblichen Systemaktualisierungen profitiert „Trixie“ unter der Haube von zahlreiche Optimierungen, die die Systemstabilität, Sicherheit und Performance verbessern. Dazu integriert die Distribution viele Patches und aktualisiert diverse Infrastrukturkomponenten, die in der langen Testphase gesammelt und verfeinert wurden. Sie booten die Live-Distribution direkt vom Datenträger, das ISO-Image finden Sie unter `isos/`. ➥ S. 74

GParted Live 1.7.0-8: Partitionsmanagement leicht gemacht

GParted dient dazu, Festplattenpartitionen ohne Datenverlust zu erstellen, zu löschen, zu verschieben, zu kopieren oder deren Größe zu ändern. Es unterstützt zahlreiche Dateisysteme wie NTFS, FAT und Ext2/3/4. Gegenüber der Vorgängerversion bringt sie vor allem Aktualisierungen der Basiskomponenten mit. Dazu gehört der Linux-Kernel in Version 6.8.9-1 mit besserer Hardwareunterstützung. Zudem wurden die zugrunde liegenden Debian-Pakete sowie Dateisystem-Tools wie E2fsprogs und Ntfs-3g auf den neuesten Stand gebracht. Sie booten die Live-Distribution vom Datenträger, das ISO-Image finden Sie unter `isos/`. (*tle*)

Darstellung symbolhaft