c't LINUX-PRAXIS

Das eigene Linux einrichten, erweitern, optimieren

System anpassen und administrieren

Überbreite und mehrere Monitore unter Gnome
Eigene Regeln definieren, Arbeit sparen

Daten sichern und wiederherstellen

Test: Quelloffene Backup-Tools mit GUI
Verlorene Dateien zurückbringen

Linux als Tonstudio

Praxis: Einführung in die Audioproduktion
Multimedia-Framework PipeWire konfigurieren

€ 14,90
CH CHF 27.90
AT € 16,40
LUX € 17,10

Windows und Linux als Dual-Boot

Windows vorbereiten • Linux neben Windows installieren
Gemeinsame verschlüsselte Datenpartition einrichten

03
4 196982 314900

Editorial

Liebe Leserinnen und Leser,

Linux auf dem Desktop ist erwachsen geworden und Ausflüge auf die Kommandozeile gehören in der Regel nicht mehr zur Pflicht, sondern zur Kür. Trotzdem schätzen Nutzer Linux für die Möglichkeit, das System zu optimieren und an die eigenen Workflows und Bedürfnisse anzupassen. c't Linux-Praxis zeigt Ihnen Stellschrauben, die Sie noch nicht gesehen haben und hilft Ihnen, mehr aus Ihrem System herauszuholen.

Nicht alle, die sich für Linux interessieren, können oder wollen Windows zurücklassen. Mit c't Linux-Praxis verheiraten Sie Windows und Linux auf einem Rechner und haben so immer das passende System für den jeweiligen Einsatzzweck. Sie lernen, wie Sie Windows sicher verkleinern und eine gemeinsame, verschlüsselte Datenpartition einrichten, damit Sie weder auf Komfort noch auf Sicherheit verzichten müssen. Wer einen Schritt weiter gehen möchte, teilt dem Bootloader Grub via USB-Stick mit, welches Betriebssystem starten soll.

Auch in puncto Display und Audio gibt es einige Szenarien, wo es sich lohnt, Hand anzulegen. Mit c't-Linux-Praxis konfigurieren Sie Ihren Desktop für mehrere oder extra große Bildschirme oder suchen mit dem Monitoring-Overlay MangoHUD nach 3D-Flaschenhälsen. Außerdem zeigen wir, wie Sie das Multimedia-Framework PipeWire konfigurieren und mit Ardour ein Tonstudio einrichten.

Backups sind immer eine gute Idee, umso mehr, wenn Sie mit dem Schraubenschlüssel im Maschinenraum Ihres Betriebssystems unterwegs sind. Beugen Sie Datenverlust vor, indem Sie eine wasserdichte Linux-Backup-Strategie entwickeln. Dazu zeigen wir, wie Sie gelöschte Dateien auf ext4-Dateisystemen zurückbringen, mit Regeln auf Events reagieren und zum SSH-Profi werden.

Viel Freude beim Linux einrichten, erweitern und optimieren!

Niklas Dierking

Inhalt

WINDOWS UND LINUX AUF EINEM RECHNER

Linux und Windows als Dual-Boot auf einem Rechner muss keine wackelige Angelegenheit sein, wenn man sich an einige Regeln hält. Mit einer gemeinsamen, verschlüsselten Datenpartition arbeiten Sie bequem weiter, egal auf welchem System Sie gerade unterwegs sind.

ANZEIGE UNTER GNOME OPTIMIEREN

Gnome gehört zu den beliebtesten Linux-Desktopumgebungen. Beim Betrieb von mehreren Displays oder Ultrawide-Monitoren offenbaren sich jedoch einige Fallstricke, die Sie mit unseren Tipps umgehen können. Als Linux-Gamer analysieren Sie mit MangoHUD die Performance Ihres Systems. Vielleicht lassen sich ja noch ein paar FPS herausholen?

LINUX ALS TONSTUDIO

Erfahren Sie, wie Sie Ihren Linux-Rechner mit Ardour zum Tonstudio machen und das moderne Multimedia-Framework PipeWire konfigurieren. Der Session- und Policy-Manager WirePlumber schafft Ordnung im Linux-Audio-Dschungel. Vereinheitlichen Sie die Benennung von Audio-Geräten, um im Videoanruf nie wieder falsche Mikrofone oder Lautsprecher zu erwischen.

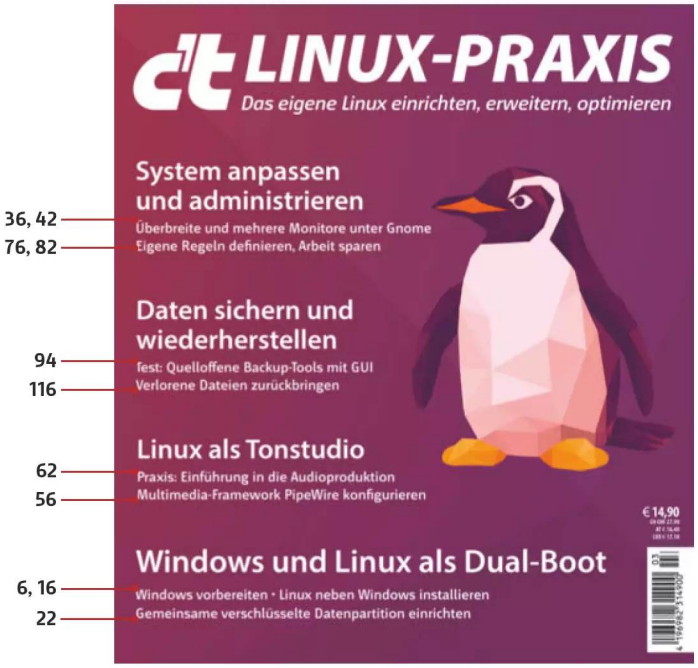
SYSTEM ANPASSEN UND ADMINISTRIEREN

Linux ist ein offenes System, passen Sie es an Ihre Bedürfnisse an! Was soll Ihr Rechner tun, wenn Sie einen USB-Stick oder ein Netzwerkkabel einstecken? Wir zeigen, wie Sie sich mit Udev-Regeln und dem NetworkManager den Linux-Alltag erleichtern und mit SSH externe Systeme administrieren. Falls Sie keine Lust auf Snap haben, dann können Sie Firefox auch mit dem Paketmanager APT installieren.

DATEN SICHERN UND WIEDERHERSTELLEN

In unserem Test vergleichen wir die Vor- und Nachteile von Backup-Tools für den Desktop, mit denen Sie Ihre persönlichen Daten sichern können. Für eine umfassende Backup-Strategie sollten Sie sich aber auch mit Backup-Live-Systemen wie Rescuezilla vertraut machen. Falls ein wichtiges Dokument mal einem Missgeschick zum Opfer fällt, lernen Sie auch, wie Sie gelöschte Dateien wiederherstellen.

ZUM HEFT



Windows oder Linux? Beides!

Wozu zwischen Linux und Windows wählen, wenn Sie von beiden profitieren können? Mit unseren Tipps verwenden Sie auf demselben PC einfach je nach Situation jenes Betriebssystem, das sich am besten eignet. Zudem speichern Sie Ihre Daten auf dem PC sicher verschlüsselt und können trotzdem von beiden Systemen gleichermaßen darauf zugreifen.

Von **Axel Vahldiek**

Bild: Sven Hauth

Geht es um die Betriebssysteme Windows und Linux, steht oft die Frage im Raum, welches der beiden denn das bessere sei. Dabei steht die Antwort seit Langem fest: Keines ist besser, sie sind nur anders. Beide haben ihre Vor- und Nachteile. So gilt Linux zu Recht als sicherer, und das nicht nur, weil es wegen seiner geringeren Verbreitung seltener angegriffen wird. Unter Windows hingegen können Sie Anwendungen nutzen, die unter Linux nicht oder allenfalls auf Krücken laufen. Doch solche Argumente sind kein Grund, ohne Not auf die Vorteile des jeweils anderen Betriebssystems zu verzichten.

Unser Vorschlag lautet daher: Nutzen Sie einfach beide Betriebssysteme. Aber nicht hermetisch voneinander abgetrennt in virtuellen Maschinen (VMs), allein schon, weil ein virtualisiert laufendes Betriebssystem nicht von der vollen Performance des Computers profitieren kann. Sondern so, dass beide Systeme mit maximalem Tempo laufen und Sie Ihre persönlichen Daten von beiden Systemen aus gleichermaßen öffnen und bearbeiten können. Und zwar ohne, dass Sie Ihre Daten erst hin- und herschaufeln müssten. So steht Ihnen für jeden Anwendungsfall stets das passende System zur Verfügung. Und zwar per Knopfdruck: Welches Betriebssystem Sie nutzen wollen, entscheiden Sie einfach beim Einschalten oder Neustart des Computers per Bootmenü.

Wenn Sie unseren Anleitungen folgen, sind Ihre persönlichen Daten zudem verschlüsselt. Das klappt selbst dann, wenn Ihre Windows-Installation ohnehin schon mit BitLocker verschlüsselt ist und Sie Linux ebenfalls verschlüsseln (siehe Artikel „Linux verschlüsseln trotz Dual-Boot“ auf S. 16).

Ob Sie als Computer einen Desktop-PC, ein Notebook oder ein Tablet verwenden, spielt keine Rolle: Ein einzelner Datenträger reicht aus, sofern er nur genug Platz bietet. Falls Windows und Ihre Daten schon drauf sind, brauchen Sie für das zusätzliche Linux nur rund 50 GByte freien Platz einzuplanen; Mehr ist nur nötig, wenn Sie große Anwendungen installieren.

Macken umgehen

Klingt alles verlockend? Prima. Zur Wahrheit gehört aber auch, dass der Parallelbetrieb von Windows und Linux nicht ganz so einfach einzurichten ist. Zwar mag so manche Anleitung suggerieren, dass es mit ein paar Mausklicks und Kaffeetrinken getan sei, doch dem ist leider nicht so. Denn auch in dieser Disziplin ist kein System das bessere: Beide bauen Mist, wenn auch unterschiedlichen: Windows fummelt später immer wieder mal ungefragt an der Aufteilung des Datenträgers herum. Die Linux-Installer wiederum ignorieren dieses Problem und schaffen mit der Brechstange Platz.

Um Linux und Windows auf demselben Datenträger zu nutzen, ist es daher der falsche Weg, den Linux-Installer einfach machen zu lassen und Daumen zu drücken. Treffen Sie stattdessen einige Vorbereitungen, und zwar unter Windows. Denn für Änderungen an der Aufteilung eines Datenträgers gilt: Bearbeiten Sie einen Bereich stets nur mit jenem Betriebssystem, zu dem er gehört. Wenn Windows weniger Platz für sich reservieren soll als bisher, dann sorgen Sie mit Windows-Bordmitteln dafür. Erst den freigeschaufelten Platz lassen Sie von Linux so einrichten, dass es sich dort wohlfühlt.

Und los!

Die Anleitungen in dieser Ausgabe helfen Ihnen durch die Einrichtung beider Betriebssysteme. Los geht es im Artikel „So verkleinern Sie die Windows-Partition“ auf Seite 8, wo wir beschreiben, wie Sie Windows so schrumpfen, dass Linux sich zusätzlich installieren lässt. Der Beitrag „Linux verschlüsseln trotz Dual-Boot“ ab Seite 16 beschreibt, wie Sie Linux verschlüsselt auf dem gleichen Datenträger installieren.

Abschließend geht es um das Entscheidende: Ihre Daten. Die lagern Sie, sofern das nicht eh schon der Fall ist, künftig getrennt vom Betriebssystem. Würden Sie die Daten auf dem Windows-Laufwerk belassen, müssten Sie später von Linux aus darauf zugreifen. Das ist eine genauso schlechte Idee wie Windows auf Linux zugreifen zu lassen. Es bestünde in beiden Fällen die Gefahr, dass ein System das andere demoliert, was Folgen bis hin zum Datenverlust haben könnte. Die Trennung vermeidet das. Zudem ist sie die Voraussetzung dafür, dass Ihre Daten ebenfalls verschlüsselt, aber für beide Betriebssysteme erreichbar sind.

Haben Sie erst mal alle Anleitungen durchgespielt, reduziert sich die seit Jahrzehnten andauernde Diskussion um das bessere Betriebssystem für Sie auf die simple Frage, welches Betriebssystem Sie beim Einschalten des Computers starten. Und die völlig undogmatische Antwort lautet: jenes, das in diesem Moment das geeignetere ist. Durch eine geteilte Datenpartition und Verschlüsselung müssen Sie trotz Dual-Boot keine Abstriche bei Komfort und Sicherheit machen. (axv) c't

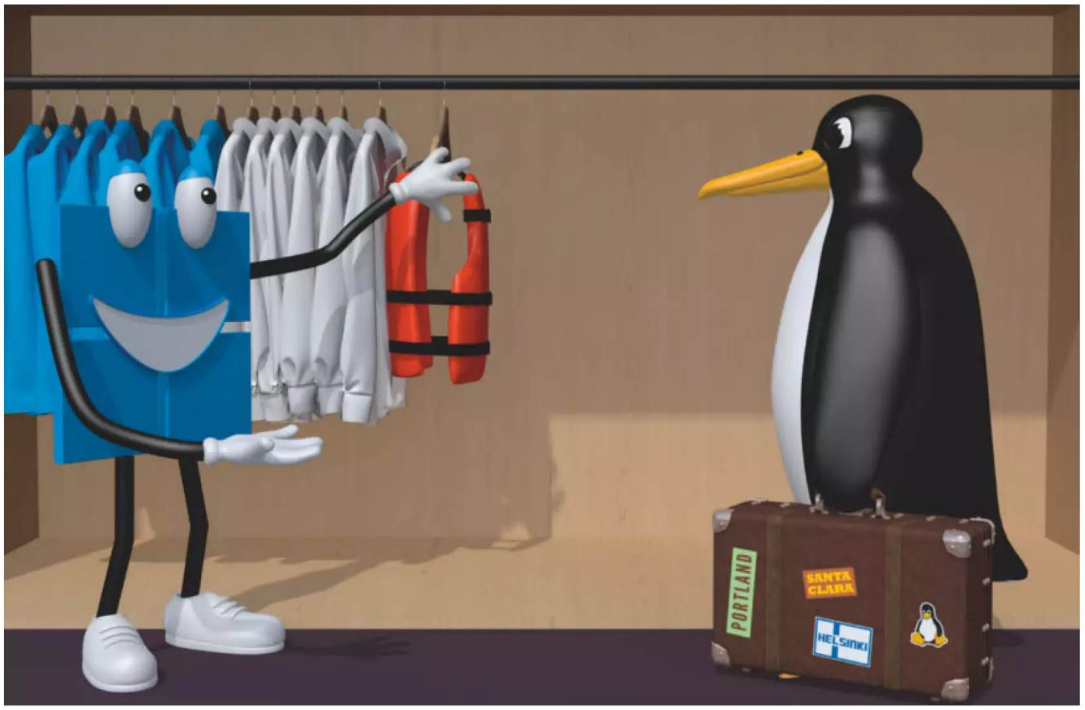


Bild: Sven Hauth

So verkleinern Sie die Windows-Partition

Der einzige Datenträger ist komplett von Windows 10 oder 11 belegt, Sie wollen aber Platz freischaufeln für Linux und/oder für Ihre Daten? Mit dieser Anleitung klappt es so, dass sich Windows und Linux anschließend auf dem Datenträger gleichermaßen wohlfühlen.

Von **Axel Vahldiek**

Der interne Datenträger in einem PC, auf dem die Windows-Installation liegt, ist standardmäßig in mehrere Partitionen unterteilt. Das sind grob gesagt logische Laufwerke. Im Explorer sehen Sie meist nur eines davon, nämlich jenes mit dem Buchstaben C:, welches die eigentliche Installation enthält. Weitere, im Explorer nicht zu sehende Partitionen enthalten beispielsweise den Bootloader oder Reparaturwerkzeuge für Notfälle, etwa wenn Windows nicht mehr bootet. Das alles getrennt zu speichern ist durchaus sinnvoll. Beispielsweise ziehen Schäden an einem logischen Laufwerk die Daten auf einem anderen nicht in Mitleidenschaft.

Wenn Sie auf dem Computer zusätzlich Linux installieren oder einen separaten Bereich für Ihre Daten schaffen wollen, auf den beide Betriebssysteme zugreifen können, bietet sich der Einbau eines zusätzlichen Datenträgers an. Doch das geht ins Geld und ist technisch nicht immer möglich: Die meisten Notebooks beispielsweise bieten in ihrem Inneren weder Platz noch Anschluss. Im Folgenden geht es darum um die Alternative: Erzeugen Sie auf dem vorhandenen Datenträger weitere logische Laufwerke. Den Platz dafür schaffen Sie, indem Sie der Windows-Installation Platz wegnehmen.

Dazu reichen an sich wenige Mausklicks. Dennoch füllt dieser Artikel mehrere Seiten, denn wenn Sie Pech haben, endet der Versuch schon im ersten Anlauf mit Fehlermeldungen. Doch selbst, wenn das Verkleinern gelingt, gibt es Nebenwirkungen, von denen Sie wissen sollten: Windows wird später an dem, was Sie da geschaffen haben, ohne Nachfrage oder Hinweis herumfummeln. Als Folge könnte ein Windows-eigenes Rettungswerkzeug in Mitleidenschaft gezogen werden, welches Ihnen eigentlich bei Boot-Problemen aus der Patsche helfen soll. Das Risiko ist zudem hoch, dass Sie das erst im Ernstfall bemerken.

Vorbereiten

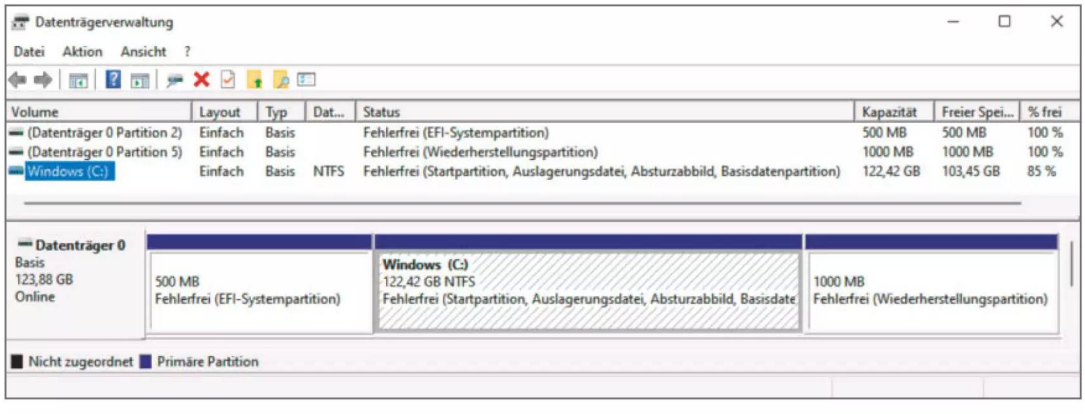
Der erste Handgriff ist derselbe wie vor vielen anderen Operationen am offenen Windows: Fertigen Sie ein Backup an. Unser Sicherungsskript c't-WIMage [1] erstellt auf einem USB-Laufwerk eine Kopie Ihrer kompletten Windows-Installation, die Sie auf quasi jeder Windows-kompatiblen Hardware wiederherstellen können. Wichtig wie bei jedem anderen Backup auch: Testen Sie nach dem Sichern, ob es wirklich geklappt hat. Alle nötigen Anleitungen und das Skript selbst finden Sie via ct.de/wimage.

Der zweite Handgriff ist optional: Schaffen Sie Platz auf C:, denn je mehr Platz dort frei ist, umso mehr können Sie von C: abknapsen. Am einfachsten gelingt das mit der Windows-eigenen Datenträgerbereinigung. Die löscht temporäre Dateien, Update-Überreste und vieles mehr. Starten können Sie sie beispielsweise, indem Sie im Eigenschaften-Dialog von C: die Schaltfläche „Bereinigen“ anklicken. Klicken Sie anschließend auf „Systemdateien bereinigen“. Dann wählen Sie kurzerhand alle Kästchen aus und lassen das Werkzeug seine Arbeit verrichten.

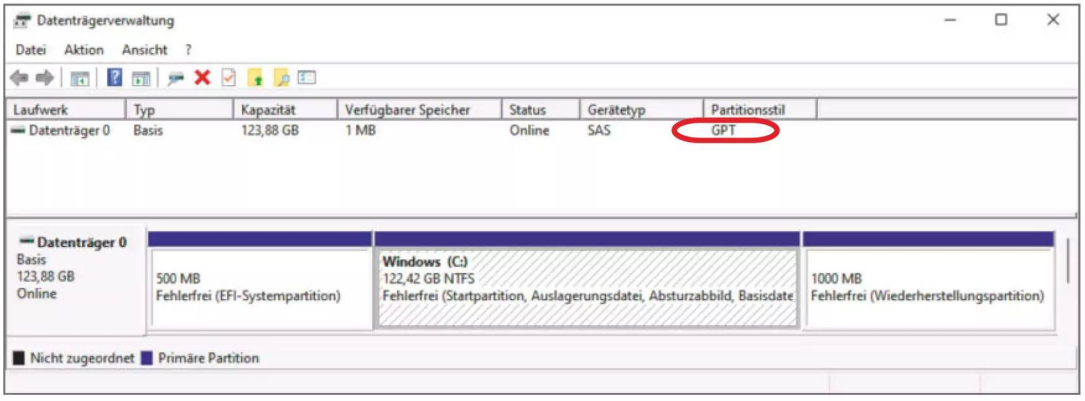
Noch nicht genug Platz frei? Öffnen Sie im Explorer Laufwerk C: und tippen Sie oben rechts in das Suchfeld `Größe:>50M` ein. Daraufhin sucht Windows alle Dateien auf C:, die größer sind als 50 MByte. Den Wert können Sie nach Belieben anpassen. Achtung: Löschen Sie von den gefundenen Dateien auf gar(!) keinen(!) Fall(!) solche, von denen Sie keine Ahnung haben, wozu sie gut sind. Denn sonst kann es passieren, dass Windows oder einzelne Anwendungen nicht mehr korrekt laufen. Entsorgen Sie also stattdessen ausschließlich, was Ihnen bekannt ist, etwa heruntergeladene Installationspakete, nicht mehr benötigte ISO-Abbilder, bereits gesehene Filme und so weiter.

Falls der Platz immer noch nicht ausreicht: Das Titelthema von c't 8/2018 bietet gleich fünf Artikel mit vielen weiteren Tipps [2].

Noch ein letzter Handgriff, bevor es wirklich losgeht: Ziehen Sie alle externen Datenträger wie USB-Platten ab, um nachfolgend die Übersichtlichkeit möglichst hoch zu halten und Verwechslungen zu



So sieht die Aufteilung eines internen Datenträgers bei einer Windows-Standardinstallation aus: Vorn die EFI-Partition mit dem Bootloader, in der Mitte die eigentliche Windows-Installation und am Ende das Rettungssystem „Windows RE“.



Wenn Sie in der Datenträgerverwaltung unter Ansicht die „Anzeige oben" auf „Datenträgerliste" umstellen, steht in der Spalte Partitionsstil bei heutigen Computern meist „GPT". Falls das bei Ihnen anders ist, kommt zusätzliche Arbeit auf Sie zu.

vermeiden. CDs und DVDs werfen sie aus. Das gilt auch für virtuell eingebundene Festplattendateien im VHD- und VHDX-Format.

Sofern C: mit BitLocker verschlüsselt ist [3], macht das nichts. Alle nachfolgend genannten Handgriffe funktionieren auch dann. Sie brauchen dafür an BitLocker also nicht herumzukonfigurieren.

Wie siehts hier denn aus?

Verschaffen Sie sich zuerst einen Überblick über die Partitionierung. Das gelingt am schnellsten mit der Windows-eigenen Datenträgerverwaltung, die unter Windows 10 und 11 gleichermaßen funktioniert (eine ausführliche Einführung haben wir in [4] veröffentlicht). Zum Starten drücken Sie die Tastenkombination Windows+X und wählen Sie den Eintrag „Datenträgerverwaltung".

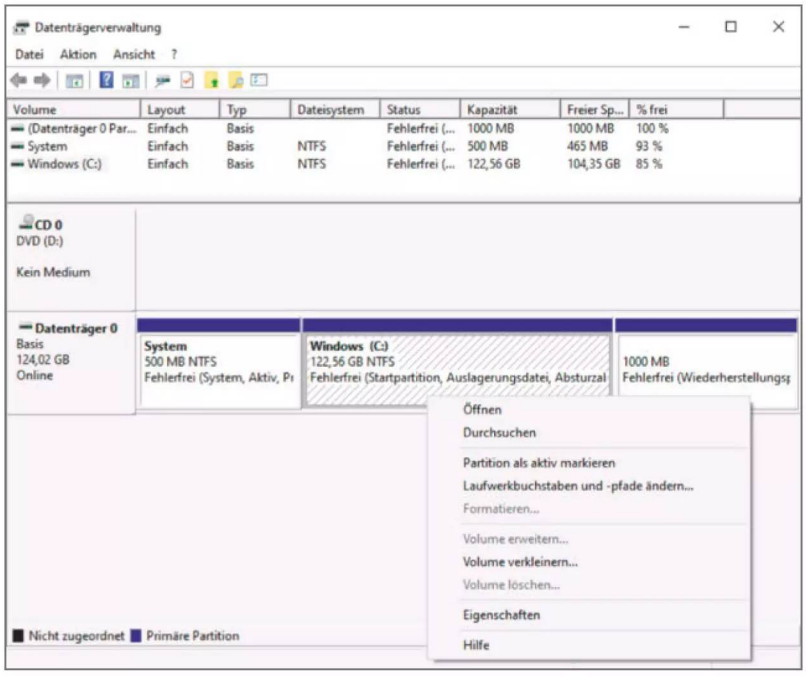
Das Programm präsentiert oben eine detaillierte Liste mit den vorhandenen Partitionen inklusive Füllstand, Art des Dateisystems, Status, ob es BitLocker-verschlüsselt ist und so weiter. Klicken Sie in der Menüleiste unter „Ansicht/Anzeige oben" auf „Datenträgerliste." In der Spalte „Partitionsstil" steht entweder „GPT" oder „MBR". Die Abkürzungen stehen für die zwei Partitionsschemata, mit denen sich die Partitionen auf einem Laufwerk verwalten lassen.

GPT ist das modernere Schema und gilt seit Jahren als Standard. Die Wahrscheinlichkeit ist daher hoch, dass Ihr Datenträger GPT-partitioniert ist, und wenn dem so ist, steht dem Platzfreischaufeln nichts im Wege. Sie können dann im Abschnitt „Schrumpfkur" weiterlesen.

Das MBR-Problem

Bei Ihnen steht „MBR"? Das ist unschön, denn MBR (veröffentlicht 1983) leidet an altersbedingten Einschränkungen. Die hier wichtigste: Es verzeichnet die Partitionen in einer Partitionstabelle, die für maximal vier Einträge Platz bietet (die „Primärpartitionen"). Weitere primäre Partitionen können Sie mit MBR nicht anlegen. Um Ihnen eigene zeitraubende Versuche zu ersparen, zuerst zu dem, was hier nicht hilft.

Das MBR-Partitionsschema kennt als Krücke die „erweiterte Partition". Mit deren Hilfe lassen sich weitere Partitionstabellen mit der ersten verketten, die jeweils Platz für maximal vier weitere logische Partitionen bieten. Das ist aber nicht empfehlenswert, allein schon, weil die erweiterte Partition einen der vier Plätze in der Tabelle benötigt. Sind derzeit alle belegt, müssten Sie also zuerst eine der vorhandenen Partitionen löschen und dazu vorab die Daten von dieser Partition wegsichern. Zudem können Sie nicht frei wählen, welche primäre Partition Sie durch eine erweiterte ersetzen wollen. Denn beispielsweise der Bootloader muss zwingend in einer primären liegen. Kurzum: Lassen Sie das. (Für die Hartgesottenen unter Ihnen, die dennoch wissen wollen, wie sie eine erweiterte Partition anlegen: Das geht unter Windows nur mit Diskpart per `Create Partition Extended`.)



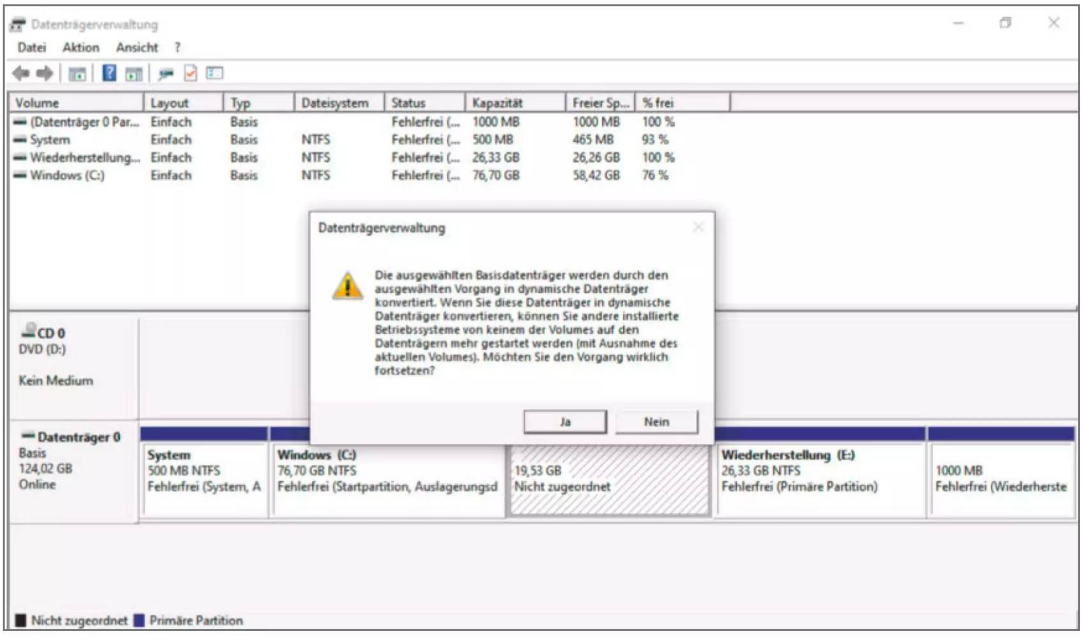
Die Datenträgerverwaltung bringt einen Assistenten zum Verkleinern der Windows-Partition mit. Der Haken ist die RE-Partition, die hier am Ende des Datenträgers liegt.

Die Datenträgerverwaltung möchte Ihnen eine andere Krücke andrehen. Wenn Sie probieren, auf einem MBR-Datenträger eine fünfte primäre Partition zu erstellen, will sie den Datenträger in einen „dynamischen“ umwandeln. Dahinter steckt im Wesentlichen eine Microsoft-eigene RAID-Lösung. Hilft nur nichts: Selbst wenn Sie auf „Ja“ klicken, wird der Datenträger trotzdem nicht umgewandelt. Stattdessen beschwert sich Windows mit einer Fehlermeldung über Platzmangel. Es fehlt ja unverändert Platz für einen weiteren Eintrag in der Partitionstabelle.

Zum Glück gibt es eine Lösung, die wirklich funktioniert: Ersetzen Sie das MBR-Partitionsschema durch GPT, denn damit sind mindestens 128 Partitionen verwaltbar. Der Haken: Mit dem Umstellen von MBR auf GPT allein ist es nicht getan. Der PC muss anschließend auch UEFI- statt Legacy-BIOS-Mechanismen zum Hochfahren nutzen, sonst bootet Windows nicht mehr. Zwei Methoden zum Umstellen haben wir in c’t bereits vorgestellt, was aber jeweils einen ganzen Artikel füllte. Die erste: Windows hat das Kommandozeilenwerkzeug „MBR2GPT.exe“ an Bord, mit dem das Vorhaben gelingt – jedenfalls dann, wenn diverse Voraussetzungen erfüllt sind und Sie einige Bugs umschiffen [5]. Die zweite: Verwenden Sie unser bereits erwähntes Sicherungsskript c’t-WIMage. Dann springt im Rahmen der Umstellung auch gleich noch eine Sicherungskopie Ihrer Windows-Installation für Sie heraus. Wie die Umstellung mit c’t-WIMage gelingt, steht ausführlich in [6].

Schrumpfkur

Nun zum Verkleinern der Windows-Partition. Das erledigen Sie in der Datenträgerverwaltung. Wählen Sie in der unteren Fensterhälfte „Volume Verkleinern …“ aus dem Kontextmenü der Windows-Partition. Falls Sie sich wundern, warum Windows scheinbar



Wenn auf dem Datenträger das alte Partitionsschema MBR verwendet wird, kann das Erstellen einer weiteren Partition scheitern. Die Datenträgerverwaltung hilft dann nicht weiter.

identische Bereiche des physischen Datenträgers mal als „Partition“ und mal als „Volume“ bezeichnet: Eine Partition belegt einen ganzen oder nur einen Teil eines physischen Datenträgers, kann sich aber nicht über mehrere erstrecken. Eine Partition enthält wiederum ein Volume, wobei es sich um das eigentliche logische Laufwerk handelt. In den meisten Fällen füllt ein Volume eine komplette Partition. Doch es kann sich auch über mehrere Partitionen erstrecken, die sogar wie bei einem RAID oder Storage Space auf unterschiedlichen Datenträgern liegen dürfen.

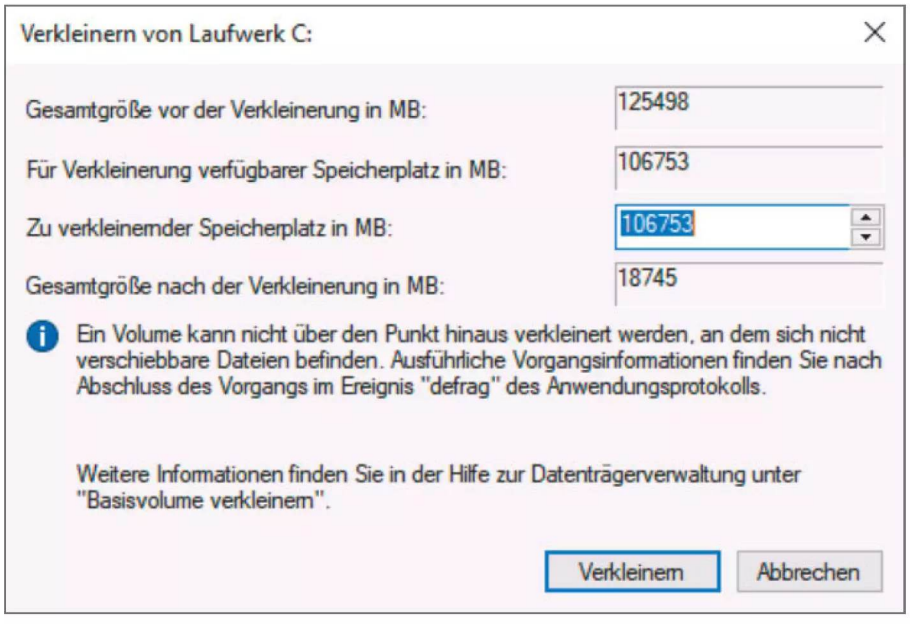
Nach dem Anklicken von „Volume verkleinern“ startet ein Assistent, der mehrere Werte anzeigt, von denen Sie einen verändern können: „Zu verkleinernder Speicherplatz in MB“. Sie wählen also nicht die Zielgröße des Laufwerks, sondern die Anzahl an MByte, die am hinteren Ende abgeschnitten werden. Der Assistent bietet den Maximalwert an, der vom Füllstand abhängt (die zu Windows-7-Zeiten geltende Beschränkung auf maximal die Hälfte spielt heute keine Rolle mehr).

Wie weit Sie das Windows-Volume verkleinern, hängt von zweierlei ab: Erstens muss Windows hinterher noch draufpassen. Wie viel Platz die Installation belegt, können Sie im Explorer in den Eigenschaften von C: ablesen. Doch dieser Platz allein reicht nicht: Windows braucht zusätzlich im laufenden Betrieb freien Platz beispielsweise für temporäre Dateien und Updates, und das gilt auch für viele Anwendungen. Als Minimum dafür gelten 20 GByte, ziehen Sie also im Assistenten vom vorgegebenen Maximalwert mindestens 20.000 MByte ab. Wenn es möglich ist, reduzieren Sie den Wert weiter. Mehr als 100 GByte freier Platz auf der Windows-Partition ist aber unnötig. Grübeln Sie über den Wert lieber eine Minute länger als zu kurz, denn nachträgliche Änderungen sind zwar machbar, aber nur mit viel Aufwand.

Sie haben einen zufriedenstellenden Wert eingetragen? Ein Klick auf „Verkleinern“ lässt den Assistenten die Schrumpfkur erledigen. In der Datenträgerverwaltung erscheint nun hinter der verkleinerten Windows-Partition ein Bereich „Nicht zugeordnet“ mit einem schwarzen Balken darüber.

Das RE-Problem

An sich können Sie den gerade freigeschaufelten Platz seiner neuen Bestimmung zuführen. Doch



Der Assistent zum Verkleinern will nicht die Zielgröße wissen, sondern um wie viele MBytes die Partition verkleinert werden soll.

lesen Sie stattdessen besser erst noch diesen Abschnitt. Denn außer der Windows-Partition gibt es noch eine weitere, die Ihrer Aufmerksamkeit bedarf. Sie enthält die Wiederherstellungsumgebung „Windows RE“ (Recovery Environment, [7]), von der Sie üblicherweise nur dann etwas bemerken, wenn Windows Probleme beim Booten hat. Bei RE handelt es sich um ein eigenständiges kleines Betriebssystem, welches der Bootloader bei Problemen automatisch startet. Es liegt in einer separaten Partition, die hier nachfolgend RE-Partition heißt.

Wie Windows selbst entwickelt Microsoft auch Windows RE immer weiter, und wie Windows wird auch RE immer größer. Als Folge wächst auch die separate RE-Partition – wenn nicht jetzt, dann irgendwann in der Zukunft, und zwar jeweils im Rahmen eines Versions-Upgrades. Die finden derzeit ungefähr jährlich statt. Wenn es so weit ist, passt Windows die Partitionierung im laufenden Betrieb an. Was dabei herauskommt, hängt von diversen Faktoren ab, die zu erläutern hier zu weit führt (Details in [8]). Scheitert Windows beim Anpassen, startet RE schlimmstenfalls nach einem Versionssprung gar nicht mehr oder nur dann, wenn C: nicht mit BitLocker verschlüsselt ist. Auch Defekte des Bootmenüs des Bootloaders sind denkbar, vor allem bei der Installation eines weiteren Betriebssystems, dessen Entwickler RE und seine Besonderheiten nicht berücksichtigen. Es können zudem zusätzliche Partitionen entstehen, die Platz verschwenden.

Damit Windows beim Vergrößern der RE-Partition nicht scheitert, muss die RE-Partition direkt hinter der Windows-Partition liegen. Dann kann Windows bei Bedarf die RE-Partition löschen, die Windows-Partition etwas verkleinern und in dem so entstandenen freien Platz hinter der Windows-Partition eine neue, nun eben etwas größere RE-Partition anlegen. Die liegt dann wieder direkt hinter der Windows-Partition.

RE verschieben

Zuerst in Kurzform, was zu tun ist, um Probleme mit der RE-Partition zu vermeiden: Deaktivieren Sie RE, woraufhin das komplette Mini-Betriebssystem vorübergehend von der RE- auf die Windows-Partition verschoben wird (es besteht ohnehin nur aus einer einzigen Datei, die beim Start von RE vorübergehend ins RAM entpackt wird). Erstellen Sie hinter der bereits geschrumpften Windows- eine neue RE-Partition und löschen Sie die alte. Zum Ab-

schluss reaktivieren Sie RE, woraufhin es funktionstüchtig an seinem neuen Speicherplatz landet.

Nun zur Langform. Das Prozedere erfordert nicht nur Mausklicks, sondern auch einzutippende Kommandozeilenbefehle. Über ct.de/wmhn finden Sie eine kleine Textdatei, aus der Sie alle Befehle herauskopieren können. Das Nachfolgende geht davon aus, dass Sie die Windows-Partition bereits wie oben beschrieben geschrumpft haben. Falls nicht, holen Sie das zuerst nach.

Los geht es in der Datenträgerverwaltung: Sehen Sie nach, auf welchem Datenträger die Windows-Partition liegt. Das erkennen Sie ganz links an der Bezeichnung „Datenträger X“, wobei X für eine Zahl steht, beginnend bei 0. Merken Sie sich die Zahl, die hinter „Datenträger“ steht.

Drücken Sie Windows+X. Wählen Sie aus dem Systemmenü je nachdem, was da ist: „Eingabeaufforderung (Administrator)“, „PowerShell (Administrator)“ oder „Terminal (Administrator)“. Tippen Sie darin den Befehl ein:

```
Reagentc /disable
```

Der Befehl deaktiviert RE. Sollte es dabei zu Fehlermeldungen kommen, liegt das üblicherweise nicht an der RE-Partition, sondern an Windows RE selbst. Hilfe und viele Tipps zum Beheben solcher Probleme finden Sie dann in [9].

Starten Sie den Kommandozeilenpartitionierer Diskpart (Einführung in [10]):

```
Diskpart
```

Wählen Sie den Datenträger mit der Windows-Partition, die Zahl ersetzen Sie durch die, die Sie in der Datenträgerverwaltung abgelesen haben:

```
Select Disk 0
```

Die nächsten beiden Befehle erzeugen eine rund 1 GByte große Partition mit dem Dateisystem NTFS und der eindeutigen Bezeichnung „ctRecovery“:

```
Create Partition Primary ↵
↳Size=1000
Format Quick FS=NTFS ↵
↳Label="ctRecovery"
```

Die Bezeichnung können Sie frei wählen, wichtig ist nur, dass sie eindeutig ist. Das hilft später beim Identifizieren und Löschen der alten RE-Partition.

Damit Windows die neue Partition als RE-Partition erkennt, passen die folgenden zwei Befehle den Partitionstyp an (hier für GPT):

```
Set ID=de94bba4-06d1-4d40↵
↳-a16a-bfd50179d6ac
GPT Attributes=0x8000000000000001
```

Sollte der Datenträger entgegen unserer Empfehlung noch MBR-partitioniert sein, reicht stattdessen ein einzelner Befehl: `Set ID=27`.

Alte RE-Partition löschen

Nun können Sie die alte RE-Partition löschen. Dazu benötigen Sie ebenfalls Diskpart. Verschaffen Sie sich zuerst einen Überblick über die vorhandenen Partitionen:

```
List Partition
```

Suchen Sie in der Liste nach Partitionen mit Namen wie „Wiederherstellung“ oder „Recovery“. Bei einer solchen kann es sich um die alte RE-Partition handeln, muss aber nicht. Auf PCs mit vom Hersteller vorkonfigurierten Windows sind oft weitere Partitionen mit ähnlichen oder gar identischen Namen vorhanden. Die enthalten beispielsweise hersteller-eigene Wiederherstellungswerkzeuge, die vom Windows-eigenen RE unabhängig funktionieren, oder Installationspakete der mitgelieferten Anwendungen und Treiber für den Fall, dass der Kunde selbst Windows neu installieren will. Images zum Wiederherstellen des Auslieferungszustands legten PC-Hersteller früher ebenfalls gern in separaten Partitionen ab, gesehen haben wir sowas aber schon länger nicht mehr.

Die alte RE-Partition erkennen Sie am Namen, am Dateisystem NTFS und an der Größe von rund 1 bis 2 GByte oder kleiner – Wiederherstellungspartitionen der PC-Hersteller sind um ein Vielfaches größer.

Der Befehl `List Partition` listet für jede Partition eine Nummer auf (ab 1 hochzählend). Suchen Sie die für die alte RE-Partition. Folgende Befehle wählen sie aus und zeigen deren Details an (X an die Partitionsnummer anpassen):

```
Select Partition X
Detail Partition
```

Steht nach dem Abschicken des zweiten Befehls in der Ausgabe eine Zeile namens `Typ: de94bba4-06d1-4d40-a16a-bfd50179d6ac` und weiter unten eine ande-

Literatur

[1] Axel Vahldiek, Ersatzrad, c't-WIMage erstellt Windows-Backups, c't 10/2021, S. 18

[2] Axel Vahldiek, Windows entschlacken, Titelthema von c't 8/2018, S. 66

[3] Jan Schüßler, FAQ: BitLocker, c't 17/2018, S. 173, auch kostenlos online lesbar unter ct.de/-4122147

[4] Axel Vahldiek, Plattenteiler, Partitionieren mit Windows-Bordmitteln – Teil 1: Datenträgerverwaltung, c't 2/2018, S. 154

[5] Axel Vahldiek, Anders hochfahren, Windows 10 von klassischem Start auf UEFI-Boot umstellen, c't 14/2019, S. 162

[6] Axel Vahldiek, Starker Helfer, PC-Umzug mit c't-WIMage, c't 6/2019, S. 22

[7] Axel Vahldiek, Aufstehhelfer, Wie Windows Startprobleme selber löst, c't 5/2018, S. 74

[8] Axel Vahldiek, Wo ist sie, und wenn ja, wie oft?, Windows RE und die Recovery-Partition, c't 18/2021, S. 162

[9] Axel Vahldiek, Hilfe für den Helfer, Windows RE prüfen und reparieren, c't 5/2018, S. 80

[10] Axel Vahldiek, Tipp-Schnippler, Partitionieren mit Windows-Bordmitteln – Teil 2: Diskpart, c't 3/2018, S. 144

re (!) Bezeichnung als die oben von Ihnen vergebene „ctRecovery“, haben Sie die richtige Partition erwischt. Diese kryptische Typ-ID ist auf GPT-Datenträgern RE-Partitionen vorbehalten (bei MBR-Datenträgern steht hier stattdessen `Typ: 27`).

Sie löschen die alte RE-Partition mit diesem Befehl (X an die Partitionsnummer anpassen):

```
Delete Partition Override
```

Lag die alte Partition bislang vor Windows, entsteht dort freier, aber nicht nutzbarer Platz, woran sich mit Windows-Bordmitteln leider nichts ändern lässt. Nun beenden Sie Diskpart durch Eingabe von `Exit` und reaktivieren Windows RE durch Eingabe von `Reagentc /enable`. Ob das geklappt hat, offenbart `Reagentc /info`, bei Problemen sei erneut auf [8] verwiesen.

Befehle.txt
ct.de/wmhn

(Fast) fertig

Das Wesentliche ist geschafft: Die Windows-Partition ist geschrumpft und die RE-Partition liegt trotzdem wieder direkt dahinter. Die nächsten Handgriffe hängen von Ihrem Vorhaben ab.

Soll der freie Platz lediglich zur Aufnahme einer separaten Datenpartition dienen, öffnen Sie ein weiteres Mal die Datenträgerverwaltung. In der unteren Fensterhälfte finden Sie im Kontextmenü des leeren, mit einem schwarzen Balken markierten Rechtecks den Eintrag „Neues einfaches Volume ...“. Ein Klick darauf startet einen weiteren Assistenten, in dem Sie nacheinander die Größe, den künftigen Laufwerksbuchstaben und die „Volumebezeichnung“ festlegen können.

Alles andere wie das Dateisystem (NTFS) ist sinnvoll vorbelegt, für Änderungen sollten Sie einen guten Grund kennen (Neugier ist keiner). Wenn der Assistent fertig ist, ist das neue logische Laufwerk bereit.

Wie Sie nun Linux verschlüsselt neben dem Windows installieren und mit unserem VeraCrypt-Setup eine gemeinsame verschlüsselte NTFS-Partition für Daten einrichten, erfahren Sie in den beiden nachfolgenden Artikeln. (axv) c't

Bild: Sven Hauth

Linux verschlüsseln trotz Dual-Boot

Ein voll verschlüsseltes Dateisystem schützt Ihre sensiblen Daten auf Notebook und Desktop selbst bei einem Diebstahl des Computers. Bei der Linux-Installation gelingt das aber nur, wenn sich Linux auf der ganzen Festplatte breitmachen darf. Wir verraten Ihnen die nötigen Kniffe, mit denen sich Debian und Ubuntu harmonisch neben Windows einfügen und trotzdem ihre Dateisysteme verschlüsseln.

Von **Mirko Dölle**

Verschlüsselte Betriebssysteminstallationen gehören heute zum guten Ton, so gelangen selbst bei Diebstahl des Computers keine Daten in die falschen Hände. Viele Linux-Distributionen bieten seit Langem voll verschlüsselte Installationen an, jedoch nur dann, wenn sie die gesamte Festplatte für sich beanspruchen dürfen – so auch bei den Installationsprogrammen von Debian 11 und Ubuntu 22.04. Haben Sie Windows parallel installiert, müssen Sie entweder auf die Verschlüsselung verzichten oder sich der nachfolgend beschriebenen Tricks bedienen.

Während es beim eher spartanischen Debian genügt, sich im Installer ein paar Mal im Kreis zu drehen, müssen Sie sich beim ansonsten komfortableren Ubuntu auf der Kommandozeile abmühen, damit

sich Linux geschmeidig neben Windows einfügt und trotzdem die Partitionen als LUKS (Linux Unified Key Setup) verschlüsselt. Da Windows auf praktisch allen Rechnern vorinstalliert ist, beginnen Sie damit, Ihre Windows-Installation zu verkleinern und so Platz für Linux zu schaffen. Dazu sollten Sie unbedingt die im Artikel „So verkleinern Sie die Windows-Partition“ auf Seite 8 beschriebene Methode mit Windows-Bordmitteln verwenden und nicht etwa das Partitionierungsprogramm Gparted unter Linux – denn bei Letzterem würden Sie einen Keil zwischen Windows und das Recovery-System treiben.

Damit ergibt sich die unten gezeigte Aufteilung der Festplatte respektive SSD: Am Anfang steht die EFI-Boot-Partition, die Windows und Linux gemeinsam nutzen, dahinter Windows und RE. Wollen Sie später auf Ihre Daten sowohl von Linux und Windows aus zugreifen, wie dies im Artikel „Gemeinsame sichere Partition einrichten“ auf Seite 22 beschrieben ist, folgt hinter den beiden Windows-Partitionen die Datenpartition. Dahinter schaffen Sie dann freien, nicht zugeordneten Platz für Linux.

Wie viel Platz Sie für Linux benötigen, hängt sehr von der späteren Nutzung ab. Weniger als 50 GByte sollten es nicht sein, auch dann nicht, wenn Sie wie im Artikel „Gemeinsame sichere Partition einrichten“ auf Seite 22 beschrieben eine gemeinsame Datenpartition für den Großteil Ihrer Dateien benutzen. Wollen Sie später Spiele installieren, müssen Sie das in jedem Fall einkalkulieren – manche benötigen 100 GByte und mehr für die Installation.

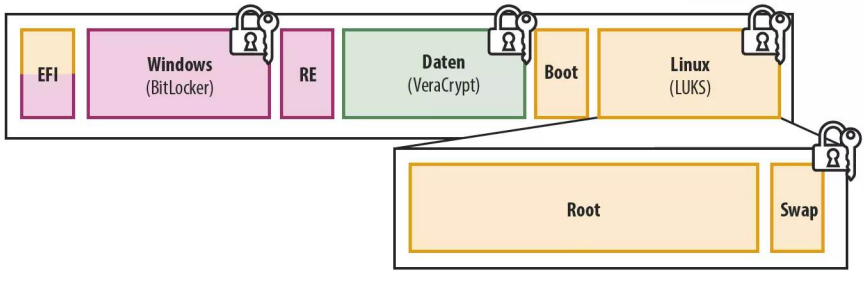
Der Knackpunkt bei der Partitionierung besteht darin, dass Debian und Ubuntu eine verschlüsselte LVM-Gruppe (Logical Volume Management) benutzen, um alle für den Betrieb benötigten (logischen) Laufwerke anzulegen. Dazu gehören mindestens das Root-Dateisystem und Swap, der Auslagerungsbereich für das RAM. So muss beim Start nur eine Partition entschlüsselt werden, die mit der LVM-Gruppe. Das wiederum erfordert, dass Bootloader Grub, Kernel und die Initial Ramdisk (initrd) auf einer unverschlüsselten Boot-Partition gespeichert sind. Ohne Unterstützung durch die Installationsprogramme müssen Sie die korrekte Partitionierung Schritt für Schritt selbst anlegen. Dies ist absurderweise beim wenig ausgefeilten Debian-Installer einfacher als unter Ubuntu.

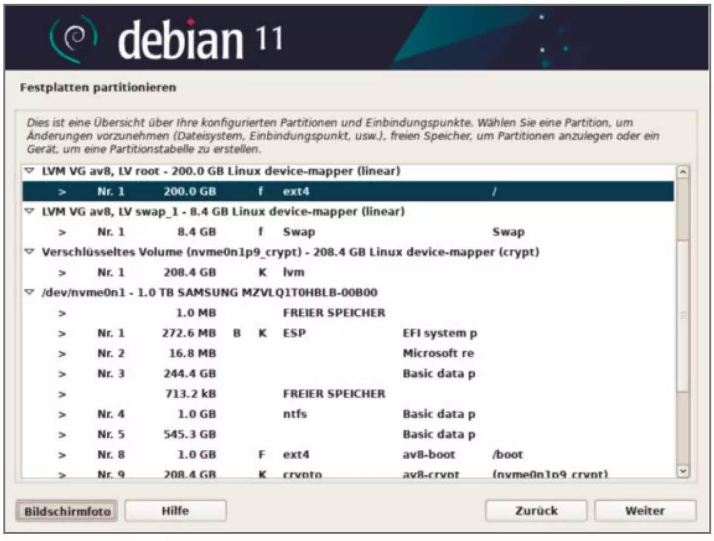
Startschuss für Debian

Bei der Debian-Installation folgen Sie einfach dem vorgezeichneten Weg so weit, bis Sie gefragt werden, wo Debian installiert werden soll. Da der Installer die Installation mit einem verschlüsselten LVM nur für den Fall anbietet, wenn Sie die ganze Festplatte für Debian benutzen, wählen Sie hier „Manuell“ aus und finden sich in der Übersicht der Partitionen wieder.

WinLin-Partitionierung

Da Windows standardmäßig installiert ist, steht es am Anfang der Festplatte, gleich hinter der EFI-Boot-Partition. Linux gehört erst hinter eine etwaige gemeinsam genutzte Datenpartition und benötigt zwei Partitionen: eine Boot-Partition und eine für das verschlüsselte mit dem Rest der Linux-Installation.





Vor und zurück, vor und zurück: Bis Sie alle für ein verschlüsseltes Debian-System benötigten Partitionen und Laufwerke angelegt haben, landen Sie immer wieder in der Übersicht der Partitionen.

Die nächsten Schritte führen Sie immer wieder zurück zu dieser Übersicht. Manchmal gibt es mehrere Optionen mit scheinbar der gleichen Funktion, folgen Sie dann bitte unserer Anleitung – sonst müssen Sie die Installation schlimmstenfalls wiederholen.

Der erste Schritt ist, eine Boot-Partition im freien Speicherbereich hinter Windows anzulegen. Diese sollte 1 GByte groß sein, damit Platz für mehrere Kernel-Versionen ist. Als Dateisystem verwenden Sie ext4, der Einbindepunkt ist /boot und als Namen sollten Sie den Hostnamen Ihres Rechners gefolgt von „-boot“ verwenden. Also zum Beispiel „debian-boot“, falls Sie den Standard-Hostnamen übernommen haben. Indem Sie möglichst alle Partitionen benennen, behalten Sie leichter den Überblick.

Zurück in der Übersicht der Partitionen wählen Sie den Menüpunkt „Verschlüsselte Datenträger konfigurieren“, um die Partition für die LVM-Gruppe zu erstellen. Dort wählen Sie den freien Bereich hinter der gerade erstellten Boot-Partition aus, die sie leicht am Dateisystem ext4 in der Liste erkennen. Als Namen empfehlen wir den Hostnamen plus „-crypt“. Erst wenn Sie die Änderungen auf die Festplatte schreiben lassen und „Fertigstellen“ ausgewählt haben, fragt der Installer das Passwort ab und verschlüsselt die Partition. Und wieder landen Sie in der Übersicht der Partitionen, wo die gerade angelegte Partition mit dem Typ „crypto“ aufgeführt ist.

Verschlüsselt, logisch?

Nun können Sie den „Logical Volume Manager konfigurieren“. Auch die „Übersicht der aktuellen LVM-Konfiguration“ werden Sie ebenfalls mehrfach betreten müssen; der erste Schritt besteht darin, eine „Volume-Gruppe“ zu erstellen. Darin sollten Sie wiederum den Hostnamen Ihres Rechners verwenden – denn das tut auch der Debian-Installer, wenn Sie die ganze Festplatte verschlüsseln lassen. Als physisches Laufwerk für das LVM wählen Sie die gerade erstellte Crypto-Partition aus, die Sie an dem Namenszusatz „-crypt“ erkennen – sie steht normalerweise am Anfang der Liste.

Damit landen Sie erneut in der LVM-Übersicht, wo Sie nun den Eintrag „Logisches Volume erstellen“ vorfinden. Das erste logische Laufwerk, das Sie anlegen, ist für das Root-Dateisystem. Dazu wählen Sie die gerade erstellte Volume Group aus und geben dem logischen Laufwerk den Namen „root“. Bei der Größe sollten Sie mindestens 8192 MByte (8 GByte) für Swap abziehen.

Und wieder landen Sie in der Übersicht der LVM-Konfiguration, wo Sie den noch freien Platz in ein weiteres logisches Laufwerk stecken, diesmal mit dem Namen „swap_1“. Das Laufwerk könnte auch anders heißen, „swap_1“ ist jedoch der Name, den der Debian-Installer standardmäßig für den ersten Auslagerungsbereich bei einer verschlüsselten Installation verwendet.

Die Einrichtung des verschlüsselten LVM ist damit komplett, weshalb Sie sie über „Fertigstellen“ verlassen und schon wieder zur Übersicht der Partitionen zurückkehren. Allerdings weiß der Debian-Installer noch nicht, was er mit den logischen Laufwerken anfangen soll. Deshalb wählen Sie zunächst aus der Liste das logische Laufwerk für Swap aus, klicken auf „Weiter“ und stellen bei „Benutzen als“ „Auslagerungsspeicher (Swap)“ ein.

Jetzt fehlt nur noch das Root-Dateisystem: Zurück in der Übersicht wählen Sie das logische Laufwerk „root“ und klicken wiederum auf „Weiter“, um es als „Ext4“ zu verwenden. Als „Einbindungspunkt“ suchen Sie „/“ aus der Liste heraus und geben der neuen Partition den Hostnamen gefolgt von „-root“, analog zur Boot-Partition.

Damit ist der schwierige Teil der Installation abgeschlossen. Klicken Sie auf „Partitionierung beenden und Änderungen übernehmen“ und dann auf „Weiter“, um den Installer den Rest der Arbeit erledigen zu lassen. Den Abschluss der Debian-Installation bildet ein Neustart, woraufhin Sie dann die Wahl zwischen Debian und Windows haben.

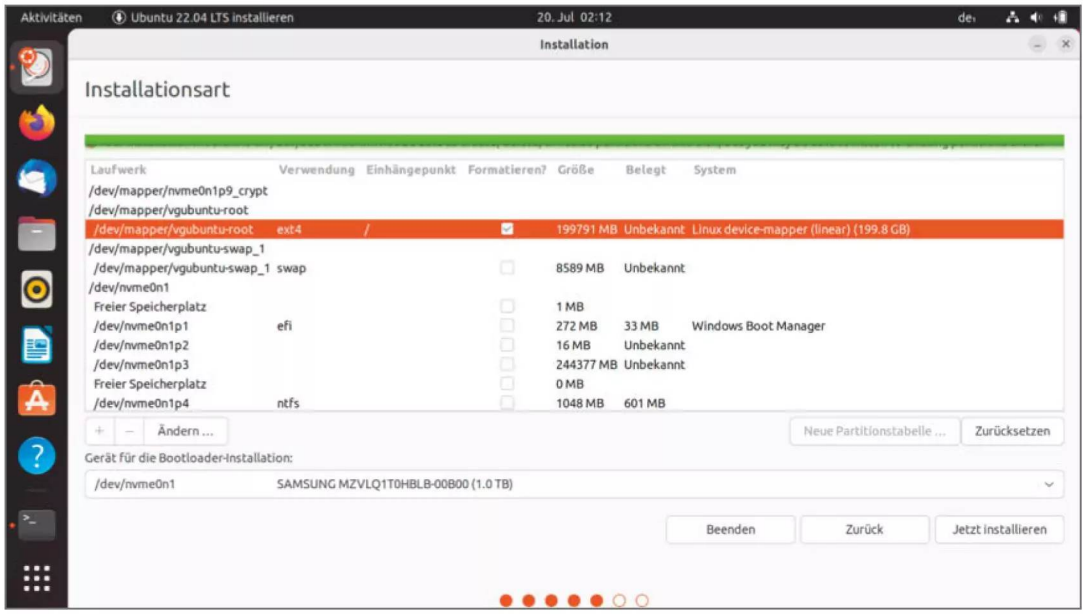
Handarbeit bei Ubuntu

Die Ursache für den Mehraufwand bei der Ubuntu-Installation liegt darin, dass der Ubuntu-Installer bei der manuellen Partitionierung kein LVM unterstützt. Diesen Teil der Arbeit müssen Sie deshalb von Hand im Terminal erledigen. Außerdem bekommt der Installer nicht mit, dass Sie ein verschlüsseltes System einrichten, weshalb Sie auch konfigurieren müssen, dass das Root-Dateisystem beim Booten erst entschlüsselt wird.

Doch der Reihe nach: Wenn Sie Ubuntu vom USB-Stick starten, wählen Sie unbedingt „Ubuntu ausprobieren“ – nur so können Sie in den Installationsprozess eingreifen und zu gegebener Zeit das LVM über das Terminal von Hand konfigurieren. Am Desktop angekommen starten Sie die Installation und folgen dem vorgezeichneten Weg, bis Sie auswählen sollen, wo Ubuntu installiert werden soll.

Komfort gibt es nur, wenn Sie Ubuntu unverschlüsselt oder auf der ganzen Festplatte installieren lassen. Deshalb wählen Sie „Etwas Anderes“ und kümmern sich anschließend selbst um die Partitionierung. Die EFI-Boot-Partition hat Windows bereits angelegt, damit müssen Sie sich nicht weiter befassen. Allerdings benötigt Ubuntu eine eigene Boot-Partition, wir empfehlen dafür mindestens 1 GByte. Lassen Sie sie mit dem Dateisystem ext4 formatieren und unter /boot einbinden.

Im nächsten Schritt legen Sie die Partition für das verschlüsselte Linux-System an. Dabei ist entscheidend, dass Sie unter „Benutzen als“ „physikalisches



Der Ubuntu-Installer erlaubt es nicht, ein LVM von Hand einzurichten – weshalb Sie diese Schritte im Terminal erledigen müssen. Gibt es ein solches LVM, erkennt es der Installer und erlaubt Ihnen auch, es einzubinden.

Volume für Verschlüsselung“ auswählen. Daraufhin erweitert sich der Dialog um die Passphrase-Abfrage. Sobald Sie den Dialog mit „OK“ bestätigen, verschlüsselt der Installer die Partition unmittelbar, bindet sie unterhalb von /dev/mapper ein und schickt Sie zurück zur Übersicht der Partitionen.

Auf Befehl

Es dauert bis zu einer halben Minute, bis die Partitionstabelle aktualisiert ist und das verschlüsselte Dateisystem als erster Eintrag in der Liste auftaucht. Nun ist es an der Zeit, das Terminal-Programm zu öffnen und das LVM einzurichten. Beginnen Sie damit, die Volume Group `vgubuntu` anzulegen:

```
sudo vgcreate vgubuntu /dev/mapper/*_crypt
```

Wie viel Platz Sie im LVM haben, verrät Ihnen der Befehl `pvdisplay --units m` in ganzen Megabytes. Ziehen Sie davon mindestens 8192 MByte für Swap ab, den Rest können Sie mit dem Logical Volume für das Root-Dateisystem belegen:

```
sudo lvcreate -n root \
  -L 200000m vgubuntu
```

Was noch frei ist, stecken Sie in das Volume „swap_1“:

```
sudo lvcreate -n swap_1 \
  -l 100%free vgubuntu
```

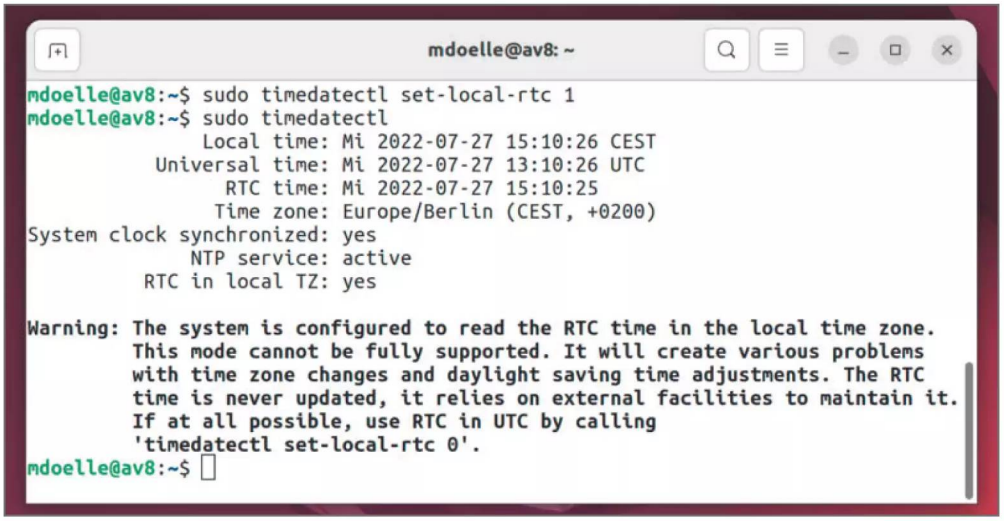
Damit die Einstellungen wirksam werden, übernehmen Sie sie mit dem Befehl `sudo vgchange -ay` und kehren zum Installer zurück.

In der Partitionsübersicht des Installers klicken Sie nun auf „Zurück“, womit Sie wieder bei der Frage landen, wo Sie Ubuntu installieren wollen. Wählen Sie dort erneut „Etwas Anderes“ und klicken Sie auf „Weiter“ – so erzwingen Sie, dass der Installer die Partitionierung aktualisiert und auch das LVM erkennt.

Nun tauchen am Anfang der Liste auch die gerade angelegten logischen Volumes auf. Indem Sie auf den Eintrag „vgubuntu-root“ respektive „vgubuntu-swap_1“ und dann auf „Ändern“ klicken, lassen Sie das Root-Dateisystem als „Ext4-Journaling-Dateisystem“ formatieren und unter „/“ einbinden; bei Swap müssen Sie lediglich „Auslagerungsspeicher (Swap)“ wählen.

Nachgeholfen

Vergessen Sie nicht, die Boot-Partition noch einmal als „Ext4-Journaling-Dateisystem“ zu formatieren und unter „/boot“ einbinden zu lassen: Weil Sie den Partitionierungsdialog verlassen hatten, hat der Installer Ihre früheren Angaben verworfen. Da sich der Installer auch nicht gemerkt hat, dass Sie mit einem verschlüsselten System arbeiten, trägt er die LUKS-Partition auch nicht in der Datei /etc/crypttab auf dem neuen System ein. Als Folge ignoriert das neu installierte System beim Booten die verschlüsselte



Während Windows standardmäßig die Lokalzeit im Rechner speichert, benutzt Linux UTC. Dies lässt sich aber leicht ändern, sodass beide Betriebssysteme stets mit der richtigen Uhrzeit booten und nicht ständig an der Uhr drehen.

Partition, findet kein Root-Dateisystem und kann deshalb nicht starten.

Dieses Problem müssen Sie ebenfalls im Terminal lösen, und zwar während der Installer das neu installierte System noch bearbeitet. Klicken Sie auf „Jetzt installieren“ und bestätigen Sie die Änderungen noch einmal. Während der Installer nun im Hintergrund Dateien kopiert und Pakete installiert, fragt er bereits die Zeitzone ab. Warten Sie einige Minuten, bis die Aktivitäten auf der Festplatte abnehmen. Dann wechseln Sie noch einmal ins Terminal, wo Sie in der crypttab die UUID der verschlüsselten Partition eintragen.

Die UUID besorgen Sie sich zum Beispiel mit dem Befehl

```
sudo blkid /dev/sda3
```

falls Sie /dev/sda3 als „physikalisches Volume für Verschlüsselung“ ausgewählt hatten.

Das Root-Dateisystem des neuen Ubuntu ist während der Installation unterhalb des Verzeichnisses /target eingebunden. Mit dem Befehl `sudo pico /target/etc/crypttab` legt der Editor Pico die Datei neu an und Sie tragen dort folgende Zeile ein:

```
sda3_crypt UUID=21e8...cf15 ↵
↳none luks,discard
```

Ist /dev/sda3 nicht Ihre verschlüsselte Partition, müssen Sie den Namen „sda3_crypt“ anpassen – er beginnt stets mit dem Partitionsnamen und endet mit „_crypt“. Die UUID haben wir nur verkürzt abgedruckt, da Ihre ohnehin eine andere ist. Den Rest der Zeile übernehmen Sie 1:1.

Speichern Sie die Datei mit Strg+O, raus aus dem Editor geht es mit Strg+X. Anschließend müssen Sie im Terminal mit folgenden Befehlen die „Initial Ramdisk“ neu bauen lassen:

```
for d in dev sys proc; do
  sudo mount --bind /${d} /target/${d}
done
sudo chroot /target \
  update-initramfs -k all -c
for d in dev sys proc; do
  sudo umount /target/${d}
done
```

Etwaige Meldungen über fehlende Firmware-Dateien können Sie ignorieren. Danach können Sie das Terminal schließen. Zurück im Installer folgen Sie den Dialogen, bis die Installation abgeschlossen ist. Haben Sie den Rechner neu gestartet, empfängt Sie Ihr nun schlüsselfertiges Ubuntu mit der Frage nach dem Passwort Ihres Systems.

Zeitreise

Ein ständiges Ärgernis bei Parallelinstallationen ist, dass Windows und Linux ständig die interne Uhr des Rechners verstellen: Windows speichert standardmäßig die Lokalzeit in der Hardware-Uhr, auch RTC (Real Time Clock) genannt, während Linux standardmäßig die Uhrzeit der Zeitzone UTC speichert. Letzteres lässt sich aber leicht mit dem Programm `timedatectl` ändern. Dazu öffnen Sie ein Terminal und geben folgenden Befehl ein:

```
sudo timedatectl set-local-rtc 1
```

Anschließend sollten Sie noch die Systemzeit, die in der Standardinstallation mit Zeitservern im Internet abgeglichen wird, in die Hardware-Uhr übertragen:

```
sudo hwclock -w
```

Ob Ihre Hardware-Uhr tatsächlich auf Lokalzeit umgestellt wurde, können Sie anschließend mit dem Befehl `sudo timedatectl` überprüfen. So vermeiden Sie, dass Windows und Linux ständig mit der falschen Uhrzeit starten und dies erst im laufenden Betrieb korrigieren. Die Warnung, dass es mit der Lokalzeit Probleme etwa bei der Sommer- und Winterzeitumstellung geben könnte, spielt auf Desktop-Rechnern keine Rolle: Das käme allenfalls zum Tragen, wenn Sie während der Zeitumstellung neu booten – und auch dann nur für wenige Minuten, bis die Systemzeit online abgeglichen und damit korrigiert wird.

Fazit

Die Installer von Debian, Ubuntu und anderen Distributionen haben klar ein Defizit, Linux verschlüsselt neben Windows installieren zu können. Indem man die schwierigen Passagen Schritt für Schritt mit ihnen durchläuft, gelingt es aber trotzdem – bei Debian sogar ohne Eingriffe im Terminal, sofern Sie unserer Anleitung penibel folgen. Vielleicht animiert dieser Artikel die Entwickler ja dazu, ihre Installer um die wenigen fehlenden Pirouetten zu ergänzen, damit sich Linux künftig ohne großen Zinnober neben Windows einfügt. (mid) c't

Bild: Sven Hauth

Gemeinsame sichere Partition einrichten

Videobearbeitung unter Windows, Server-Administration unter Linux, Surfen und E-Mails überall: Mit einer gemeinsamen Datenpartition können Sie für jede Aufgabe die am besten geeignete Anwendung nutzen. Mit unserem VeraCrypt-Setup werden Ihre Daten zudem automatisch ver- und entschlüsselt, ohne dass Sie sich ein Passwort merken müssen.

Von **Mirko Dölle**

Obwohl Windows und Linux unterschiedliche Dateisysteme benötigen und verschiedene Verschlüsselungstechniken einsetzen, bedeutet die Parallelinstallation nicht zwangsläufig doppelte Datenhaltung. Mit VeraCrypt und NTFS gibt es einen gemeinsamen Nenner für eine verschlüsselte Datenpartition, mit der beide Betriebssysteme zurechtkommen. So vermissen Sie nie wieder Hör-

bücher, die Sie unter Windows heruntergeladen hatten, wenn Sie unter Linux programmieren oder Server warten.

Dieser Artikel beschreibt, wie Sie die gemeinsame Datenhalde durch angepasste Standardpfade und symbolische Links so in die Desktop-Umgebungen beider Betriebssysteme einbinden, dass Ihre Bilder, Dokumente, Downloads, Musik und Videos standardmäßig auf der gemeinsam genutzten Partition landen und diese beim Systemstart auch ohne zusätzliche Eingabe eines Passworts eingebunden wird. So verhält sich die Datenpartition transparent, Sie bekommen kaum mit, dass es sie überhaupt gibt, und können unter beiden Betriebssystemen wie gewohnt arbeiten.

Wir haben uns für VeraCrypt entschieden, weil sich das Programm unter Linux und für Windows bewährt hat. Mit der Einrichtung einer VeraCrypt-verschlüsselten Datenpartition beginnen Sie idealerweise, nachdem Sie wie im Artikel „So verkleinern Sie die Windows-Partition“ auf Seite 8 beschrieben Windows verkleinert haben: Öffnen Sie erneut die Datenträgerverwaltung von Windows, klicken Sie mit der rechten Maustaste auf den zuvor freigegebenen Speicherbereich und wählen Sie aus dem Kontextmenü „Neues einfaches Volume...“ aus. Bedenken Sie bei der Größe der künftigen Datenhalde, dass Sie ja noch Platz für die Linux-Installation benötigen – 50 GByte sollten das mindestens sein, mit vielen Anwendungen besser 100 GByte. Falls Sie viele native Linux-Anwendungen oder Spiele installieren wollen, brauchen Sie vielleicht noch mehr. Was Sie nicht für Linux benötigen, geben Sie der neuen Partition und wählen „Keinen Laufwerksbuchstaben oder -pfad zuweisen“ sowie „Dieses Volume nicht formatieren“, damit Windows die Partition in Ruhe lässt und nicht etwa zusätzlich mit BitLocker verschlüsselt.

Als Nächstes laden Sie die Windows-Version der kostenlosen Verschlüsselungssoftware VeraCrypt von veracrypt.fr herunter und installieren diese mit den Standardeinstellungen. Den Abschluss bildet ein Neustart von Windows, danach starten Sie VeraCrypt zum ersten Mal.

Fast unsichtbar

Damit VeraCrypt später nahezu unsichtbar arbeitet und die Datenpartition automatisch einbindet, verwenden Sie anstatt eines Passworts einen Schlüssel zum Entschlüsseln; der ist auf der mit BitLocker oder ebenfalls mit VeraCrypt verschlüsselten Windows-Systempartition und später auf der LUKS-verschlüsselten Linux-Partition sicher aufgehoben. Diesen Schlüssel erzeugen Sie über das Menü „Tools/Keyfile Generator“ und speichern ihn etwa unter dem Namen „winlin-key“ im persönlichen Ordner des Administrators. Anschließend kopieren Sie den Schlüssel mit dem Explorer auf einen USB-Stick, um ihn später unter Linux einlesen zu können.

Über „Tools/Volume Creation Wizard“ verschlüsseln Sie die zuvor angelegte Datenpartition, indem Sie dort „Encrypt a non-system partition/drive“ auswählen und ein „Standard VeraCrypt volume“ anlegen lassen. Als „Volume Location“ wählen Sie die Partition aus und klicken anschließend auf „Create encrypted volume and format it“. Wenn VeraCrypt nach dem „Volume Password“ fragt, lassen Sie das leer und aktivieren stattdessen „Use keyfiles“ und wählen unter „Keyfiles...“ die zuvor erzeugte Schlüsseldatei winlin-key aus. Bei der Frage nach „Large Files“ sollten Sie „Yes“ auswählen und bei „Volume Format“ als „Filesystem“ „NTFS“, außerdem „Quick Format“, damit VeraCrypt den Speicherbereich nicht überschreibt. Sofern sich dort zuvor Ihre mit BitLocker verschlüsselte Windows-Partition befunden hat, ist die Schnellformatierung kein Problem – dort lagerten dann keine Klartext-Daten.

Haben Sie die Partition mit VeraCrypt verschlüsselt und formatiert, wählen Sie dafür einen Laufwerksbuchstaben aus – zum Beispiel V:. Keinesfalls sollten Sie D: oder einen anderen vom Anfang des Alphabets nehmen, der zukünftig einem USB-Stick oder Kartenleser zugeordnet werden könnte, denn dann laufen später die neuen Standardpfade ins Leere. Als „Volume“ wählen Sie über „Select Device...“ die gerade vorbereitete Partition aus und klicken dann auf „Auto-Mount Devices“, damit die Partition künftig bei jedem Start von Windows wieder entschlüsselt und eingebunden wird. Wählen Sie bei der Passwortabfrage wiederum „Use keyfiles“ und unter „Key“ winlin-key als Schlüsseldatei aus.

Um die Datenpartition künftig automatisch bei jedem Systemstart einbinden zu lassen, klicken Sie mit der rechten Maustaste in der Liste der Laufwerksbuchstaben auf V: und wählen „Add to Favourites...“ aus dem Kontextmenü. Aktivieren Sie in der Liste der Optionen „Mount selected volume upon logon“ sowie „Mount selected volume when its host device gets connected“.

Damit VeraCrypt Sie zukünftig nicht mehr mit der Frage nach dem Passwort oder der Schlüsseldatei behelligt, importieren Sie über „Settings/Default Keyfiles...“ und dort über „Add Files...“ den Schlüssel

winlin-key als Standardschlüssel. Außerdem aktivieren Sie die Option „Try first to mount with an empty password“, ansonsten erwartet VeraCrypt später weiterhin eine manuelle Passworteingabe. Damit ist das Einrichten der verschlüsselten Datenpartition unter Windows abgeschlossen.

Auf neuen Pfaden

Wenn Sie die Windows-eigenen Ordner für Bilder, Downloads und so weiter verwenden, können Sie diese auf die VeraCrypt-Partition verlegen. Zum Ändern der Standardpfade legen Sie zunächst mit dem Explorer auf der VeraCrypt-Partition einzelne Verzeichnisse für Bilder, Dokumente, Musik, Videos und Downloads an. Den Desktop dürfen Sie dort nicht speichern, denn dieser baut sich unter Umständen schon auf, noch bevor die Partition eingebunden ist – das führt dann zu hässlichen Fehlermeldungen.

Um den Standardpfad für Bilder auf V:\Bilder zu ändern, klicken Sie im Explorer mit der rechten Maustaste im linken Navigationsbereich unterhalb von „Dieser PC“ auf „Bilder“ und wählen aus dem Kontext-Menü „Eigenschaften“. Im Register „Pfad“ klicken Sie nun auf „Verschieben“ und wählen das Verzeichnis V:\Bilder als neuen Ort aus. Sobald Sie auf „Übernehmen“ klicken, fragt Sie der Explorer, ob er die vorhandenen Daten dorthin verschieben soll – sagen Sie „Ja“. Genauso gehen Sie mit allen anderen Ordnern vor, die Sie auf die gemeinsame Datenpartition verlegen wollen. Jetzt ist Ihre gemeinsame Datenpartition voll integriert.

Bei der Einrichtung unter Linux haben Sie die Wahl zwischen VeraCrypt mit GUI, womit Sie dann auch komfortabel USB-Sticks verschlüsseln können, und der reinen Kommandozeilenversion – die genügt, um die Datenpartition einzubinden, die Verwaltung von Partitionen sollten Sie besser unter Windows erledigen. VeraCrypt spielen Sie aber erst ein, nachdem Sie bereits Linux verschlüsselt neben Windows und neben der bereits eingerichteten Datenpartition installiert haben. Der Artikel „Linux verschlüsseln trotz Dual-Boot“ auf Seite 16 beschreibt, worauf Sie bei Debian 11 und Ubuntu 22.04 LTS achten müssen. Die nachfolgende Anleitung zur Einrichtung von VeraCrypt gilt für beide Distributionen.

Linux schlüsselfertig

Laden Sie sich das zu Ihrer Distribution passende Paket, mit oder ohne GUI, aus dem Download-Bereich von veracrypt.fr herunter. Danach öffnen Sie ein Terminal, um es mit folgenden Befehlen zu installieren:

```
sudo dpkg -i Downloads/veracrypt*.deb
sudo apt -f install
```

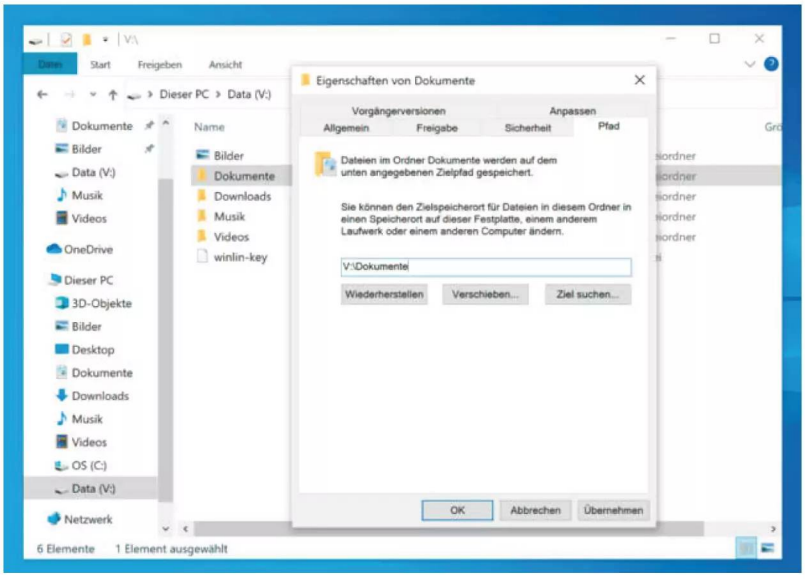
Der zweite Befehl dient dazu, die Paketabhängigkeiten automatisch aufzulösen. Im nächsten Schritt legen Sie den Mount Point für die Datenpartition an, außerdem ein Verzeichnis für Schlüssel und kopieren dann den VeraCrypt-Schlüssel winlin-key vom USB-Stick in das neue Verzeichnis:

```
sudo mkdir /data
sudo mkdir -m 700 /etc/crypto
sudo cp /media/*/*/winlin-key \
  /etc/crypto
```

Automagie

Damit ist VeraCrypt betriebsbereit und Sie können sich darum kümmern, dass die Datenpartition künftig beim Systemstart automatisch entschlüsselt und eingebunden wird. Dazu ergänzen Sie folgende Zeile am Ende der Datei /etc/crypttab:

```
winlin-data /dev/sda3 /dev/null ↵
↳tcrypt-veracrypt,tcrypt-keyfile=↵
↳/etc/crypto/winlin-key
```



Indem Sie die Standardpfade auf die gemeinsam genutzte Datenpartition verschieben, sind Ihre Bilder, Dokumente, Downloads und vieles mehr auch unter Linux abrufbar.

Den Gerätenamen /dev/sda3 ersetzen Sie durch den Gerätenamen Ihrer Datenpartition, den Sie mit dem Befehl lsblk herausfinden. Damit wird die Datenpartition entsperrt und bekommt den Namen „winlin-data“. Die folgende Zeile am Ende der Datei /etc/fstab bindet die Datenpartition schließlich unterhalb von /data ein:

```
/dev/mapper/winlin-data /data auto ↵
↳uid=1000,gid=1000,nodev,nofail 0 0
```

Nach dem nächsten Neustart ist die Datenpartition für den ersten Benutzer im System mit der User-ID 1000 beschreibbar unter /data eingebunden. Verschieben Sie nun den Inhalt des Verzeichnisses „Bilder“ in Ihrem „Persönlichen Ordner“ (Home-Verzeichnis) nach /data/Bilder, etwa per Drag & Drop mit zwei Fenstern des Dateimanagers Nautilus.

Anschließend löschen Sie das nun leere Verzeichnis Bilder. Um einen symbolischen Link zum Bilderverzeichnis auf der gemeinsamen Datenhalde anzulegen, ziehen Sie das Verzeichnis /data/Bilder aus dem anderen Nautilus-Fenster per Drag & Drop in Ihren „Persönlichen Ordner“ und halten dabei die Alt-Taste gedrückt. Beim Loslassen wählen Sie dann aus dem Kontextmenü „Verknüpfung erstellen“. Damit verweist der Ordner Bilder in Ihrem Home-Verzeichnis auf das Verzeichnis /data/Bilder, wo auch Ihre Bilder aus Windows gespeichert sind. Diesen Vorgang wiederholen Sie für Dokumente, Musik, Videos und alle anderen Verzeichnisse, deren Daten Sie künftig auf der gemeinsamen Datenpartition speichern wollen.

Welche Anwendung wofür?

Zwei verschlüsselte Betriebssysteme mit gemeinsamer Datenpartition sind eine tolle Arbeitsgrundlage – doch womit arbeitet man konkret? Das hängt davon ab, was Sie individuell benötigen oder wo Ihre Vorlieben liegen. Falls Sie regelmäßig mit Kollegen an MS-Office-Dokumenten oder Präsentationen arbeiten, werden Sie nicht an Microsoft Office unter Windows vorbeikommen. Unter Linux genügt Ihnen Libre- oder OpenOffice, mit denen Sie einen Blick in ein Office-Dokument werfen können.

Spielt Kompatibilität keine große Rolle, können Sie sich das Geld für Microsoft Office sparen und auch unter Windows zur Open-Source-Variante Ihres Linux-Office-Pakets greifen. Dann haben Sie den Vorteil, dass es keine Konvertierungsprobleme mit Ihren eigenen Office-Dateien gibt und die Bedienung weitgehend einheitlich ist.

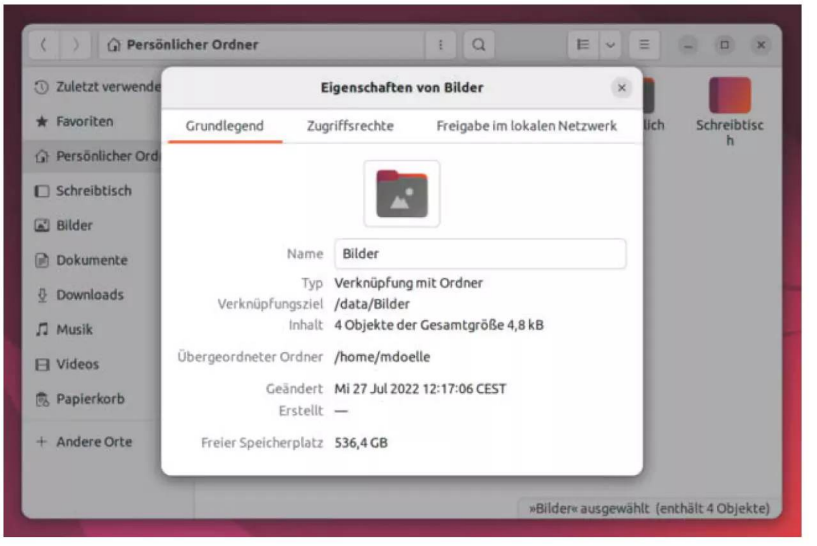
Es muss aber nicht immer das gleiche Programm sein: Falls Sie allenfalls mal den Anfang und das Ende eines Screen-Recordings wegschneiden, genügen dazu die jeweiligen Bordmittel von Windows und Linux. Erst wenn Ihre Projekte etwas ambitionierter werden, lohnt es sich, wenn Sie sich in das wesentlich leistungsfähigere Kdenlive einarbeiten, das es für beide Betriebssysteme kostenlos gibt. Videoproducer hingegen werden kaum an Adobe Premiere für Windows vorbeikommen, benötigen dann aber unter Linux keinen speziellen Videoeditor.

Ähnlich ist es bei der Foto- und Bildbearbeitung: Wer das beruflich macht oder große Ambitionen hat, wird früher oder später Photoshop und die Adobe Creative Suite benutzen müssen. Dann hat es aber wenig Sinn, sich zusätzlich in Gimp einzuarbeiten – unter Linux genügt dann die Vorschau, um sich Bilder anzusehen. Benötigen Sie hingegen nicht den Leistungsumfang eines Adobe Photoshop, kann Gimp eine Alternative für Windows und Linux sein. Auch dann profitieren Sie von der einheitlichen Bedienung.

Als Browser empfehlen wir Ihnen Firefox: Haben Sie einen kostenlosen Account angelegt, können Sie per Firefox Sync von den Lesezeichen bis hin zu den gerade geöffneten Tabs und Websites alles zwischen Windows und Linux synchronisieren, was Sie für den Alltag brauchen. Je mehr Sie synchronisieren (und damit verschlüsselt in die Cloud übertragen) lassen, desto leichter fällt es Ihnen später, ad hoc von Windows nach Linux zu wechseln und umgekehrt – denn Sie können nahtlos da weiter surfen, wo Sie auf dem anderen Betriebssystem gerade waren.

Sofern Sie Ihre E-Mails per IMAP bei Ihrem Provider abholen, können Sie genauso gut Thunderbird unter Windows und Linux einsetzen wie zwei verschiedene Programme: Wenn beide Programme die Entwürfe in dem dafür vorgesehenen IMAP-Ordner zwischenspeichern, können Sie sogar E-Mails unter Linux fertig schreiben, die Sie unter Windows begonnen haben – und umgekehrt.

Auch bei manchen Spielen haben Sie die Wahl, die Wikinger-Variante von Minecraft, Valheim, zum Beispiel gibt es im Steam Store sowohl für Windows als auch für Linux. Sie können sich für eine der beiden Varianten entscheiden, oder aber die Spielstände über die Steam Cloud zwischen Windows und Linux synchronisieren lassen. Diese Lösung ist auch besser, als aufwendig die Speicherpfade der Spielstände unter Windows und Linux so zu verändern, dass sie auf der gemeinsamen Datenpartition landen: Nicht alle Windows-Spiele kommen mit den Dateien der anderen Plattformen zurecht, die Cloud-Synchronisation von Steam hingegen ist eigens darauf ausgelegt.



Durch symbolische Links für Bilder, Dokumente und andere Verzeichnisse verweisen Sie alle Linux-Anwendungen auf die gemeinsam genutzte Datenpartition als Speicherort, sodass Sie sie auch unter Windows öffnen können.

Fazit

Man muss sich nicht zwischen Windows und Linux entscheiden. Beide Betriebssysteme haben ihre Berechtigung und sind letztlich nur die Basis, auf der man seine eigentliche Arbeit erledigt – mit dem am besten dafür geeigneten Werkzeug. Die gemeinsame verschlüsselte Datenpartition und Funktionen wie Firefox Sync machen es Ihnen leicht, für eine bestimmte Aufgabe das jeweils andere Betriebssystem zu booten und dabei an der gleichen Stelle weiterzuarbeiten, an der Sie aufgehört haben. (mid) c't

Know-How statt Hype

Mit KI-Tools effektiv arbeiten

Heft + PDF mit 29 % Rabatt

Die Nachrichten über revolutionäre KI-Lösungen überschlagen sich täglich. Wie soll man da den Überblick behalten? Mit Tests und Praxistipps erklären wir im c't-Sonderheft, was heute schon geht sowie Ihnen bei der Arbeit hilft und wo Sie den Maschinen noch Zeit zum Reifen geben sollten.

- ChatGPT zwischen wirtschaftlicher Effizienz und menschlichem Wunschdenken
- Bilder-KI Stable Diffusion lokal installieren und betreiben
- Textgeneratoren für jeden Zweck
- Sprachmodelle mit Suchmaschinen koppeln
- Vier KI-Komponisten im Test
- ChatGPT als Hacking-Tool

Heft für 14,90 € • PDF für 12,99 € • Bundle Heft + PDF 19,90 €

shop.heise.de/ct-chatgpt

Bild: Collage c't / KI Midjourney

USB-Stick wählt Windows oder Linux

Ein eingesteckter USB-Stick ersetzt das Rumtippen im Grub-Menü bei Dual-Boot-Systemen: Je nach Stick bootet das gewünschte Betriebssystem ohne Wartezeit.

Von **Rüdiger Willenberg**

Ein kurzer Tagtraum, das Grub-Bootmenü rauscht vorbei, und das falsche Betriebssystem startet. Diesen Ärger kennen Nutzer von Dual-Boot-Systemen mit Linux und Windows, die nebeneinander auf demselben Rechner installiert sind. Viele Gründe sprechen für Dual-Boot-Installationen (siehe Artikel „Windows oder Linux? Beides!“ auf S. 6 und Artikel „Linux verschlüsseln trotz Dual-Boot“ auf S. 16), beispielsweise kommen beide Systeme ohne Geschwindigkeitsnachteile an die Hardware heran. So kann Mama tagsüber mit der dicken Grafikkarte unter Linux neuronale Netze trainieren, während abends die Sprösslinge die 3D-Performance für das Gaming unter Windows abfordern. Und wer ein c't-Abo hat, wird durchaus auch mal aus reiner Neugier mit einem anderen Betriebssystem experimentieren wollen.

Die verbreitetste Lösung für Multiboot ist der Open-Source-Bootloader Grub 2. Nach dem Systemstart übergibt das UEFI-Bios ihm die Kontrolle und

er kann sowohl Windows als auch alle Linuxe starten. Die Wahl trifft man über ein textbasiertes Auswahlmenü. Da die meisten Nutzer aber ganz häufig die erste Option starten und nicht wollen, dass der Rechner ewig in diesem Menü hängen bleibt, läuft ein Timer ab, nach dessen Ablauf Grub wahlweise ein als Default eingestelltes Betriebssystem oder das zuletzt benutzte bootet. Während man sich ärgert, weil man nicht aufgepasst hat und mal wieder das falsche System gestartet hatte, fragt man sich während des Reboots: Warum kann das nicht so einfach sein wie bei einer alten Spülmaschine mit mechanischer Programmwahl?

Genau diesen Wunsch erfüllt das Projekt „The GRUB Switch“. Durch eine kleine Erweiterung des Bootskriptes grub.cfg schaut Grub auf einem USB-Speicher nach, welchen Menüeintrag es booten soll. In der einfachsten Nutzungsvariante wählen Sie durch Einstecken eines normalen USB-Sticks mit der passenden Datei das gewünschte Betriebssystem aus. Sie können sich mit einem Mikrocontroller und ein wenig Löten auch einen echten Schalter für den gleichen Zweck bauen [1].

The GRUB Switch greift sehr zurückhaltend in den Bootvorgang ein: Die eigentliche Grub-Installation wird nicht verändert (Details im Kasten „Unter der Grub-Haube“ auf Seite 32) und so besteht kein erhöhtes Risiko, den eigenen PC in einen Briefbeschwerer zu verwandeln. Findet das ergänzte Bootskript keine passende Auswahldatei, setzt es den herkömmlichen Bootvorgang fort.

Vorbereitung

Voraussetzung für eine erfolgreiche Erprobung ist eine existierende Installation, bei der das GRUB2-Bootmenü erscheint. In der Praxis ist das der Fall, wenn mindestens eines der installierten Betriebssysteme ein Linux ist. Im Minimalfall existieren keine anderen Betriebssysteme, aber Grub bietet wenigstens den „Safe Mode“ oder ältere Kernelversionen an. Auf vielen Systemen gibt es auch einen Menüpunkt für den Neustart ins UEFI-BIOS.

The GRUB Switch konfiguriert man menübasiert über die Kommandozeile in einem Linux-Terminal. Für die meisten Arbeitsschritte benötigen Sie `sudo`-Rechte, können also nach Passwortabfrage Kommandos als Administrator (Linux-Benutzer root) absetzen. Öffnen Sie ein Linux-Terminal und probieren Sie das Kommando: `sudo whoami`. Kommt nach der Passworteingabe eine Warnmeldung, dass Sie nicht in der Liste der autorisierten sudo-User sind, suchen

Bild: Pina Merkert

Ein kleiner USB-Stick im Steckplatz reicht, damit Grub ohne Wartezeit Linux bootet. Für Windows liegt ein zweiter Stick bereit. Das Menü braucht man mit „The GRUB Switch“ nur noch in Spezialfällen.

Sie in der Dokumentation Ihrer Distribution nach `sudo` und verschaffen sich die nötigen Rechte für einen zweiten Versuch nach erneutem Einloggen.

Die Software des Grub-Switch-Projekts finden Sie auf GitHub, weshalb Sie die Dateien sehr leicht mit `git` auf Ihren Rechner klonen können:

```
git clone \
https://github.com/rw-hsma-fpga/grub-switch.git
```

Falls Sie `git` nicht installieren möchten, können Sie das Projekt auch mit `wget` herunterladen und per Hand entpacken:

```
wget https://github.com/rw-hsma-fpga/↵
          ↳grub-switch/archive/refs/↵
          ↳heads/master.zip
unzip master.zip
mv grub-switch-master grub-switch
```

Danach finden Sie die Dateien des Projekts im Ordner grub-switch.

Menübasiert konfiguriert

Die Software zum Grub-Switch bringt Shellskripte mit, mit denen Sie die Bootoptionen über einfache Menüs konfigurieren. Damit Sie die Menüs ganz sehen können, sollten Sie Ihr Konsolenfenster groß ziehen, beispielsweise mit dem Maximieren-Knopf in der Titelleiste. Wechseln Sie danach mit

```
cd grub-switch/1_config_scripts
```

in das Unterverzeichnis, das alle Shellskripte zur Konfiguration enthält. Nach der Passwortabfrage bringt Sie der Befehl

```
./CONFIGURE_GRUBswitch.sh
```

in das im Bild unten dargestellte Hauptmenü. Das listet oben auf, ob und wann das Skript die Einträge des Grub-Menüs ausgelesen, Dateien für Sticks und Arduino-Micro-Hardware erstellt, Hashes berechnet hat und wann die Konfigurationsdatei grub.cfg zuletzt verändert wurde. Letztere wird nicht nur vom GRUB-Switch-Skript aktualisiert, sondern auch von den Skripten der Distribution, beispielsweise nach Kernel-Updates. Bei Elementary OS liegt die grub.cfg in einem anderen Ordner, den Sie dem Skript aber mit der Option `-g /boot/efi/EFI/ubuntu/grub/` mitteilen können. Beim ersten Start existieren die GRUB-Switch-Dateien natürlich noch nicht.

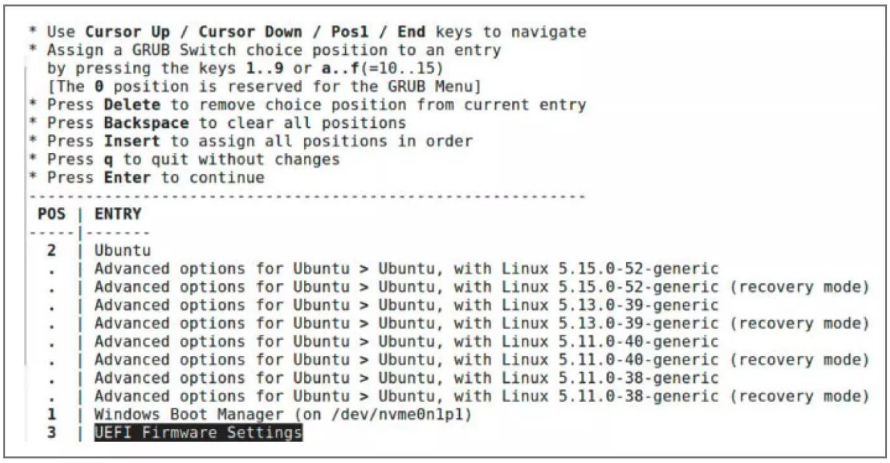
Unter den Statusangaben folgen die Aktionen, die The GRUB Switch einrichten. Sie wählen diese einfach mit den Zahlentasten aus. Es ist ausreichend, wenn Sie die Punkte 1, 2, 5 und 7 und 7 nacheinander durchlaufen.

Um die für Sie relevanten Bootmenü-Eintrage selektieren und sortieren zu können, muss das Skript zunächst eine komplette Liste aus der existierenden Grub-Konfiguration ziehen. Wählen Sie dazu mit der Taste 1 die Aktion „Extract all menu entries from grub.cfg“. Außer unter Linux Mint lassen Sie das Skript an dieser Stelle einmal grub.cfg neu erstellen, weil das auf manchen Distributionen Probleme mit automatischen Übersetzungen umgeht. Mint nutzt ein zweifelhaftes Skript beim Reboot, das die Namen noch mal tauscht. Die Daten landen in der Textdatei grub-switch/bootfiles/grubmenu_all_entries.lst. Mit einem beliebigen Tastendruck kehren Sie zum Hauptmenü zurück. Die Statusübersicht zeigt jetzt das Datum an, an dem die Menüeinträge zuletzt extrahiert wurden.

Mit 2 (Configure GRUBswitch order and generate bootfiles and hashes) starten Sie die eigentliche Konfiguration. Das Tool zeigt in Tabellenform die Auswahloptionen des Grub-Menüs. Dabei tauchen auch alle Einträge aus Untermenüs auf; in unserem Beispiel sind dies die verschiedenen Kernelversionen, die das installierte Ubuntu booten kann.

```
Status of files:
----------------

Extracted list of GRUB menu entries  (../bootfiles/grubmenu_all_entries.lst):
-> not present

Generated boot files for regular flash drives (../bootfiles/boot.[1..f]):
-> not present
Generated boot file for GRUBswitch USB device (../bootfiles/.entries.txt):
-> not present

Permitted SWITCH.GRB file hashes  (/boot/grub//grub_switch_hashes/*):
-> not present (no permission checking)

GRUB menu config file  (/boot/grub//grub.cfg):
-> last modified at 18 Okt 2022 - 16:48:07
   contains up-to-date GRUBswitch code


ACTIONS:
--------

1 - Extract all menu entries from grub.cfg
2 - Configure GRUBswitch order and generate bootfiles and hashes
3 -   Remove generated files
4 - Write GRUBswitch bootfile to GRUBswitch USB device        (requires sudo)

5 - Install up-to-date hashes for permitted SWITCH.GRB files  (requires sudo)
6 -   Remove all hashes, no permission checking               (requires sudo)

7 - Install GRUBswitch into grub.cfg                          (requires sudo)
8 -   Remove GRUBswitch from grub.cfg                         (requires sudo)

q - Quit
```

Den Grub-Switch konfigurieren Sie über Menüs, die auf einzelne Nummern oder Buchstaben reagieren. Vom hier dargestellten Hauptmenü durchlaufen Sie für den Einsatz von USB-Sticks die Punkte 1, 2, 5 und 7.



Mit der menügeführten Konfiguration wählen Sie die Einträge aus dem Grub-Menü aus, die Sie mit einem USB-Stick booten möchten.

Mit den Pfeiltasten navigieren Sie durch die Einträge. Die Tasten 1 bis 9 markieren Einträge fürs Booten per USB-Stick oder Schalter und weisen zugleich eine Auswahlposition zu. Für den seltenen Fall, dass mehr als 9 Optionen notwendig sind, stehen noch die Buchstabentasten A bis F zur Verfügung, die den Positionen 10 bis 15 in der Reihenfolge entsprechen. Die Auswahlposition 0 ist für das unveränderte Grub-Menü reserviert. Merken Sie sich die gewählte Reihenfolge, Sie brauchen sie später.

Mit dem Menü können Sie auch die aktuelle Zuweisung löschen (Entf-Taste), alle getätigten Zuweisungen löschen (Backspace), 15 Positionen in Tabellenreihenfolge zuweisen (Einfg-Taste) oder das Tool ohne Änderungen verlassen (Q). Mit einem Druck auf Enter akzeptieren Sie die aktuellen Zuweisungen und gelangen zum nächsten Schritt.

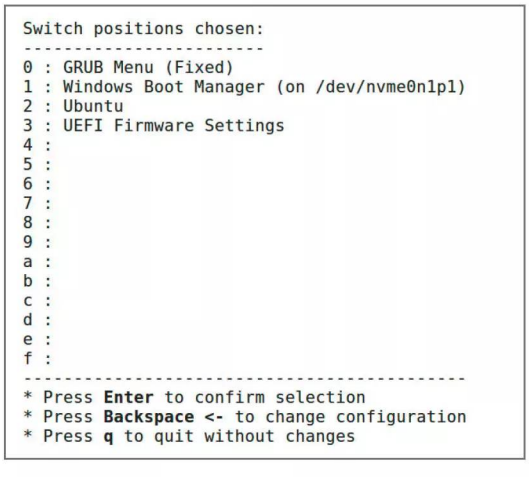
Das Konfigurationsskript zeigt Ihnen nochmals die ausgewählten Einträge in der zugewiesenen Reihenfolge.

Zur Kontrolle zeigt Grub die per Hardware ausgewählte Bootoption kurz an, bevor sie startet. Währenddessen gelangen Sie mit der Esc-Taste zum normalen Grub-Menü. Für erste Experimente ist eine Wartezeit als Absicherung und Rückmeldung hilfreich. Wenn alles läuft, können Sie die Verzögerung auf null setzen. Das nächste Menü ermöglicht, mithilfe der Cursortasten die Wartezeit einzustellen.

Haben Sie eine Wartezeit eingestellt, können Sie – rein ästhetisch – in einem Folgemenü eine Kombination aus Schriftfarbe und Hintergrundfarbe für die Anzeige des zu bootenden Systems wählen. Mit den Pfeiltasten für Links und Rechts wechseln Sie zwischen den Farbkombinationen. Achtung: Nicht alle Linux-Terminals stellen die gewählten Farben so dar, wie Grub sie später zeigt. Achten Sie im Zweifel auf die Textangabe, zum Beispiel „white/red“ für weiße Schrift auf rotem Hintergrund.

Das Konfigurationsskript gibt abschließend noch aus, wie die Konfigurationsdaten in die Datei grub-switch/bootfiles/.entries.txt geschrieben wurden, die im Folgeartikel für die selbst gelötete USB-Schalterhardware verwendet wird. Mit einem beliebigen Tastendruck kehren Sie in das Hauptmenü und zur Aktionsliste zurück.

Die Statusübersicht zeigt die Daten für die aktuell erzeugten Konfigurationsdateien. Mit der Taste



Zur Kontrolle zeigt das Konfigurationsskript ein zweites Mal eine Liste mit den ausgewählten Bootoptionen.

Unter der Grub-Haube

Um vollautomatisch mit den Update-Mechanismen verschiedenster Linux-Distributionen zu funktionieren, verwendet Grub 2 einen skriptbasierten Mechanismus. Nach dem Start des Bootloaders und noch bevor Grub sein Menü anzeigt, arbeitet es die Schritte ab, die in der Datei /boot/grub/grub.cfg festgelegt sind. Die Syntax des Skripts ist eng an die von POSIX-Shells wie `bash` angelehnt; der Sicherheit halber sind aber keine Schreibvorgänge auf die Datenträger möglich.

Bootmenü-Einstellungen wie das Default-Betriebssystem, die Wartezeit des Menüs und Textfarben setzen Umgebungsvariablen im Skript. Das wichtigste Grub-spezifische Kommando dieser Shell ist `menuentry`, das einen Menüeintrag erstellt. Zu diesem Befehl gehört jeweils ein Block von Anweisungen, die Grub bei Auswahl des Menüeintrags ausführt. Auch hierarchische Untermenüs sind damit möglich. Die nutzen Linux-Distributionen zum Beispiel, um das Booten mit älteren Kernelversionen oder im „Safe Mode“ anzubieten.

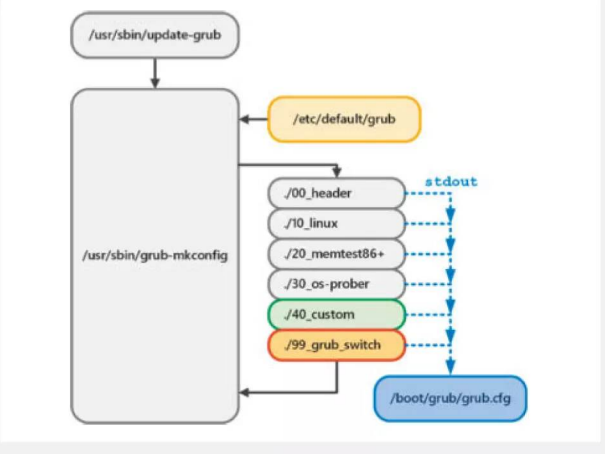
Die Vermutung liegt nahe, dass man durch Editieren von grub.cfg eigene Modifikationen vornehmen könne. Dies ist aber nicht empfehlenswert: Das Skript ist eine automatisch generierte Datei, die zum Beispiel überschrieben wird, wenn die Linux-Installation ein Kernel-Update macht. Der Mechanismus dafür ist im Bild rechts dargestellt.

Zum Neuerzeugen startet man mit root-Rechten `/usr/sbin/update-grub`. Der Aufruf bringt eine Kette mehrerer Linux-Shell-Skripte in Gang, die nacheinander ablaufen. Dabei wird auch die Konfigurationsdatei /etc/default/grub gelesen: Darin können Sie permanente Einstellungen wie GRUB_DEFAULT (die Nummer des standardmäßigen Starteintrags) und GRUB_TIMEOUT (die Wartefrist in Sekunden) setzen, die dann in grub.cfg einfließen.

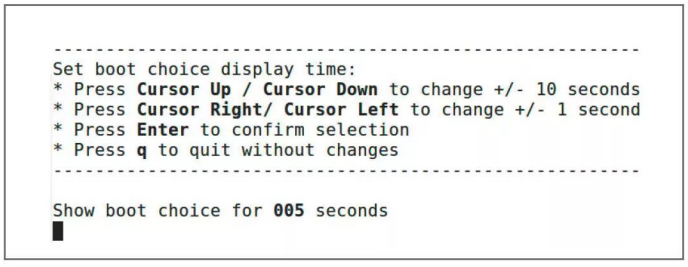
Die Skript-Kette arbeitet sich schließlich durch eine Gruppe von nummerierten Skripten im Verzeichnis /etc/grub.d/, deren Textausgabe der neu generierten grub.cfg als Code hinzugefügt wird. So entsteht auch die Zusammensetzung des Grub-Menüs, denn die benötigten `menuentry`-Kommandos werden jeweils von den zuständigen Skripten wie `10_linux` oder `30_os-prober` (findet andere Systeme wie Windows) erzeugt.

User mit Schreibzugriff auf /etc/grub.d/ können der grub.cfg ihre eigenen Befehle in eigenen Skripten hinzufügen, die dann vor der Anzeige des Grub-Menüs ausgeführt werden. Für solche Zwecke steht die Datei `40_custom` bereit, in die solcher Code eingefügt werden kann. The GRUB Switch installiert im gleichen Ordner mit `99_grub_switch` ein eigenes Skript, das den benötigten Bootschalter-Code in grub.cfg schleust. Dieser Code sucht nach einem FAT-Datenträger mit der Datei SWITCH.GRB, die dann als Skript aufgerufen wird – optional nach Sicherheitsprüfung per Hash – und die gewünschte Wahl per Umgebungsvariable setzt.

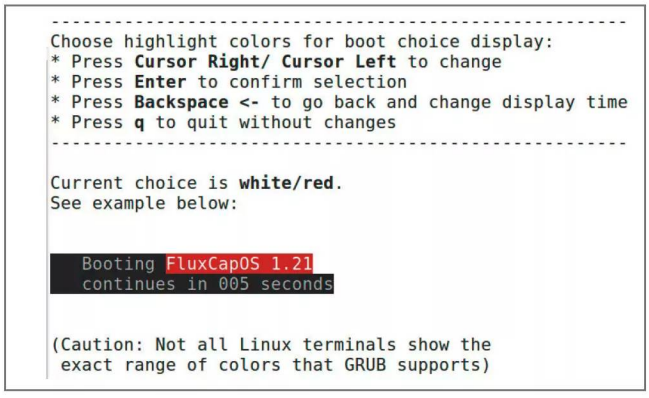
Ein Hinweis zur neuesten Grub-Version 2.06: Hier hat das Grub-Team die automatische Ausführung von `30_os-prober` deaktiviert, da die Suche nach anderen bootbaren Betriebssystemen eine Sicherheitslücke darstellen könnte. In der Praxis hat das die frustrierende Folge, dass Windows-Installationen nicht mehr erkannt und ins Menü aufgenommen würden. Ubuntu 22.04 LTS macht deswegen einen Kompromiss: Findet es bei der Systeminstallation ein Windows, so wird auch weiterhin `30_os-prober` ausgeführt. Um auf Ihrem System ganz sicherzugehen, fügen Sie in der Datei /etc/default/grub den Eintrag `GRUB_DISABLE_OS_PROBER=false` ein, sodass jeder folgende `update-grub`-Aufruf Windows berücksichtigt.



Das Skript grub-mkconfig führt alle Skripte in /etc/grub.d/ nach Namen sortiert aus. Die Reihenfolge entsteht, weil die Dateinamen mit einer zweistelligen Zahl beginnen. Die Ausgaben der Skripte schreiben gemeinsam /boot/grub/grub.cfg. Auf den meisten Distributionen stößt man den Prozess über das Skript update-grub an, das grub-mkconfig automatisch ausführt.



Zum Testen sollten Sie eine Wartezeit von einigen Sekunden einstellen, damit Sie im Notfall noch mit ESC ins normale Bootmenü kommen. Wenn alles läuft, setzen Sie die Wartezeit später auf null.



Bei mehr als null Sekunden Verzögerung dürfen Sie auswählen, in welchen Farben The GRUB Switch die per Hardware gewählte Bootoption anzeigt.

3 könnten Sie diese auch wieder komplett löschen und neu beginnen. Noch ist aber ohnehin nichts am Bootvorgang verändert.

Die eigentliche Installation passiert mit der Aktion 7 (Install GRUBswitch into grub.cfg), die dem Bootskript /boot/grub/grub.cfg den nötigen Code hinzufügt. Weil Sie dazu `sudo`-Rechte brauchen, werden Sie nach Ihrem Passwort gefragt. Geben Sie nach der Aufforderung Ihr Passwort ein und bestätigen dann mit Enter. Anschließend müssen Sie den Schreibvorgang noch einmal mit Y für „Ja" bestätigen, bevor das Skript grub.cfg mit dem hinzugefügten Code neu generiert. Ein weiterer beliebiger Tastendruck bringt Sie zum Hauptmenü zurück, das das Update nun oben beim Status anzeigt. Für die Vorbereitung der USB-Sticks verlassen Sie das Konfigurationstool nun mit Q.

USB-Sticks einrichten

Wechseln Sie mit `cd ../bootfiles` in das Verzeichnis bootfiles im Projektordner und lassen Sie sich den Inhalt mit `ls -la` anzeigen (die Option `a` zeigt auch versteckte Dateien, die sich in Linux nur durch einen führenden Punkt im Namen von anderen unterscheiden). Sie sehen unter anderem:

- Die Datei grubmenus_all_entries.lst, in die alle Grub-Menü-Einträge extrahiert wurden.
- Die schon zuvor angezeigte Datei .entries.txt, die für die kommende Arduino-Lösung benötigt wird.
- Nummerierte Unterverzeichnisse wie boot.1, boot.2, boot.3 etc., je nachdem, welche Zahlen/Buchstaben zuvor im Konfigurationstool zugewiesen wurden.

In den Unterverzeichnissen boot.X liegt jeweils eine einzige Datei SWITCH.GRB, nach der der grub.cfg-Code auf USB-Laufwerken sucht, um sie auszuführen.

Sie können sich den Inhalt einer Datei beispielhaft mit `cat boot.1/SWITCH.GRB` anzeigen lassen. Der Inhalt ist kurz erklärt: Der Shell-artige Skript-Code setzt zunächst Variablen für den gewählten Booteintrag sowie die Wartezeit und Farben für die Anzeige. Danach stellt er den jeweiligen Booteintrag als Default-Vorgabe des normalen Grub-Menüs und stellt dessen Wartezeit auf null Sekunden. Anschließend gibt Grub den Eintrag in den gewünschten Farben aus. Erfolgt kein Abbruch, kehrt das Skript zum aufrufenden Skript grub.cfg zurück. Aufgrund der vorweggenommenen Einstellungen wird das eigentliche Grub-Menü aber nicht angezeigt, sondern direkt der gesetzte Eintrag gebootet. Falls Sie die Wartephase mit Esc abbrechen, erscheint das Grub-Menü ohne Zeitbegrenzung.

Für den nächsten Schritt benötigen Sie ein oder mehrere USB-Sticks, die mit dem FAT-Dateisystem formatiert sind. Die Sticks müssen lediglich je eine SWITCH.GRB-Datei speichern, die wenige Hundert Bytes groß ist. Es kommen also auch Werbegeschenke und schnarchlangsame Uralt-Sticks in Frage. Falls Sie neu kaufen, eignen sich Mini-Sticks, die oft we-

niger als 10 Euro kosten und kaum größer als der USB-A-Stecker sind.

Für jede Bootoption stecken Sie einen Stick in den USB-Slot und binden ihn ein. Dieses Mounten erledigen moderne Linux-Distributionen automatisch. Wenn der USB-Stick danach zum Beispiel als /media/username/MYDRIVE32MB eingehängt ist, kopieren Sie die erste Auswahldatei mit

```
cp ./boot.1/SWITCH.GRB ↵
        ↳/media/username/MYDRIVE32MB/
```

darauf. Hängen Sie den Stick anschließend entweder per Mausklick oder mit `sync && sudo umount /media/username/MYDRIVE32MB` aus, damit die Datei auch tatsächlich geschrieben wird, statt im Schreibpuffer des Systems zu verweilen. Dann ziehen Sie den Stick ab und markieren Sie ihn gleich per Stift oder Aufkleber mit der gewählten Option. Wiederholen Sie den Vorgang mit allen USB-Sticks und Dateien in den Verzeichnissen boot.2, boot.3, und so weiter.

In der Minimalvariante mit zwei Betriebssystemen reicht übrigens schon ein einzelner USB-Stick, beispielsweise am Schlüsselbund, aus: Wenn eine Windows- und eine Linux-Installation auf dem Rechner warten und Windows in /etc/default/grub als Default eingestellt ist, erscheint nach dem Start das Grub-Menü und nach Ablauf der Wartezeit (auch in /etc/default/grub einstellbar) läuft Windows los. Dann brauchen Sie nur den USB-Stick mit der SWITCH.GRB für die Linux-Option.

Danach ist es Zeit, das Ganze auszuprobieren: Stecken Sie den passenden Stick in eine USB-Buchse und starten das System neu. Grub sollte Sie mit der kurzen Anzeige der passenden Bootoption begrüßen und danach das entsprechende OS starten.

Secure Boot

Falls es nicht gleich klappt, ist der Bösewicht vermutlich das UEFI-BIOS des PCs: Prüfen Sie, ob das Booten von USB-Laufwerken erlaubt ist. Der Grub-Switch bootet zwar gar nicht von USB, aber falls verboten, wird der USB-Controller nicht früh genug aktiviert. Etwas perfider ist eine Variante, über die der Autor bei seinem Lenovo-Notebook gestolpert ist: Hier wird der USB-Zugriff für Grub schon unmöglich, falls die eigentlich sinnvolle UEFI-BIOS-Option „Secure Boot“ aktiviert ist, obwohl sie mit USB auf den ersten Blick gar nichts zu tun hat. In einem solchen Fall scheint das Deaktivieren des Secure Boot leider die einzige Option, The GRUB Switch zu nutzen.

Wir haben The Grub Switch mit allen Distributionen aus dem c’t-Linux-Netzplan (siehe ct.de/wzv5) getestet und leider funktionierte nur das „echte“ Ubuntu (also nicht die Derivate Mint und Elementary) sowie OpenSUSE „Leap“ (auch nicht das Rolling-Release „Tumbleweed“) automatisch mit Secure Boot.

Falls sich bei Ihnen die Nackenhaare gesträubt haben, als Sie lasen, dass Grub versucht, eine Skriptdatei von einem eingesteckten USB-Laufwerk auszuführen, hatten Sie die richtige Intuition. Skripte ungeprüft von USB-Sticks auszuführen ist ein Einfallstor par excellence für Hacker. Um Ihren Computer gegen das Ausführen beliebiger Grub-Skripte zu sichern, bietet The GRUB Switch einen Hash-basierten Mechanismus, der nur vorher zugelassene SWITCH.GRB-Dateien ausführt.

Um den zu aktivieren, wechseln Sie ins Verzeichnis bootfiles im Projektordner. Listen Sie dort zunächst den Inhalt des Ordners grub_switch_hashes mit `ls -l grub_switch_hashes` auf. Dort gibt es zu jedem Ordner boot.1, boot.2, … eine entsprechende Datei 1.sha512, 2.sha512, …. Ein `cat grub_switch_hashes/*` zeigt alle Dateien an, was offenbart, dass jede einen SHA512-Hashcode für die korrespondierende SWITCH.GRB-Datei enthält.

GRUB kann ebenfalls solche Hashes von Dateien bilden und vergleichen: Passt der Hash einer gefundenen SWITCH.GRB-Datei nicht zu den hinterlegten, ignoriert Grub sie.

Der GRUB-Switch-Code prüft Hashes aber nur, wenn er den Ordner /boot/grub/grub_switch_hashes findet. Den lokalen Ordner mit den vom Skript erzeugten Hashes müssen Sie also an die richtige Stelle kopieren. Navigieren Sie dafür mit `cd ../1_config_scripts` zurück zum Ordner mit den Konfigurationsskripten und starten Sie das Skript erneut mit dem Befehl:

```
./CONFIGURE_GRUBswitch.sh
```

Wählen Sie im Hauptmenü die Aktion 5 (Install up-to-date hashes for permitted SWITCH.GRB files). Nach Kopieren des Hashordners und Rückkehr ins Hauptmenü mit einem beliebigen Tastendruck wird nun auch der Status der Hash-Installation mit Datum angezeigt. Falls es Probleme gibt, lässt sich der Hash-Ordner mit der Aktion 6 einfach wieder entfernen.

Praktisch sollte sich durch die zusätzliche Sicherheitsmaßnahme erst mal nichts ändern. Sie können weiterhin mit Ihren vorbereiteten USB-Sticks die verschiedenen Optionen booten, denn die Hashes passen ja. Sollte sich in einer SWITCH.GRB-Datei aber

auch nur ein Bit ändern, ergibt die Prüfung einen komplett anderen Hash und die Datei wird nicht mehr ausgeführt.

Falls Ihre Linux-Distribution überhaupt mit Secure Boot funktioniert, gibt es leider auch Probleme, die am Design von Grub liegen: Zur Hash-Berechnung muss ein Modul nachgeladen werden, das es anscheinend nicht durch die Signaturprüfung schafft; die Hashprüfung der Auswahldateien scheitert dann immer. Man muss sich in diesem Fall also leider zwischen der Deaktivierung von Secure Boot im UEFI-BIOS oder dem Verzicht auf die Hash-Prüfung und erneutem Deinstallieren des Hashordners entscheiden.

Noch gemeiner sind Probleme bei Fedora und openSUSE, die zurzeit als einzige eine ungepatchte Version von GRUB 2.06 verwenden: Fedora verweigert die Hash-Funktionen mit Ausführungsfehlern in Grubs internen C-Funktionen. Allerdings geben diese Fehler den gleichen Rückgabewert an grub.cfg wie eine erfolgreiche Hash-Prüfung – und würde damit auch falsche Skript-Dateien durchlassen. Bei openSUSE (Leap und Tumbleweed) tritt dieses Fehlverhalten nur beim standardmäßig verwendeten btrfs-Dateisystem auf – wählt man stattdessen ext4, funktioniert die Hash-Prüfung korrekt.

Fazit

Mithilfe des Projektes The GRUB Switch können Sie mittels eingestecktem USB-Stick vorauswählen, welches System Grub startet. Dank des menübasierten Konfigurationsskripts brauchen Sie zum Einrichten keine tiefgehenden Linux-Kenntnisse. Die automatischen Update-Mechanismen der Linuxe werden durch The GRUB Switch nicht gestört. Ein einzelner USB-Stick reicht, um gelegentlich zu Linux statt Windows oder andersherum abzubiegen. (pmk) c't

Literatur

[1] Pina Merkert, Arduino im Boot, Physische Schalter für The GRUB Switch bauen, c't 13/2023, S. 142

The GRUB Switch bei GitHub, Linux-Netzplan

ct.de/wzv5

Gnome-Anmeldung: Multimonitor steuern

Bei vielen Linux-Distributionen wie Ubuntu oder Fedora stellt der Gnome Display Manager (GDM) den Anmeldebildschirm bereit. Bei mehreren Monitoren entscheidet GDM automatisch, auf welchem Display die Login-Maske erscheint. Mit etwas Handarbeit kann man die Automatik beeinflussen und so für Homeoffice oder Büro Vorgaben festlegen.

Von **Keywan Tonekaboni**

Wie beim Gnome-Desktop üblich, verfolgt auch der Gnome Display Manager (GDM) die Philosophie, Anwender möglichst nicht mit Konfigurationen zu behelligen. In den grafischen Systemeinstellungen findet man abgesehen von der automatischen Anmeldung praktisch keine Optionen, um den GDM anzupassen. Meist besteht dafür auch kein Bedarf. Selbst komplexere Display-Konfigurationen mit mehreren und wechselnden Monitoren erkennt GDM in der Regel und passt die Ausgabe an das vorgefundene Setup an, wobei es die Monitore automatisch anordnet.

Doch hier offenbart GDM auch eine Macke: Es zeigt die Login-Maske nur auf dem primären Bildschirm an. Je nachdem, welches angeschlossene Gerät GDM dazu auserkoren hat, kann die Anmeldung zum Suchspiel mutieren. Wenn etwa die Wahl auf das eingebaute Display des Laptops fällt, dieser aber zugeklappt in der Dockingstation schlummert. Auch um 90° gedrehte Bildschirme bindet GDM verkehrt ein, da der Bildinhalt nicht rotiert wird. In den grafischen Systemeinstellungen gibt es keine Möglichkeit, auf die Anordnung Einfluss zu nehmen. Wir zeigen Ihnen in dieser Praxisanleitung, wie es mit einem versteckten Trick trotzdem klappt. Mit ein paar Kommandozeilenbefehlen und etwas XML-Grundwissen schieben Sie die Login-Maske von GDM auf das gewünschte Ausgabegerät – und das auch für verschiedene Szenarien, etwa für Büro, Homeoffice und den Beamer im Wohnzimmer.

Vorbereitung

Warum GDM nicht einfach die Systemeinstellungen übernimmt, hängt damit zusammen, wie Gnome die Monitorkonfiguration verwaltet. Wenn Sie in Gnome die Anzeigeeinstellungen ändern, beispielsweise die Auflösung oder Anordnung der Monitore, dann erzeugt die Gnome-Shell innerhalb Ihres Homeverzeichnisses im Ordner .config die Konfigurationsdatei monitors.xml (~/.config/monitors.xml). Falls Sie die Datei nicht finden können, haben Sie vermutlich Ihre Anzeigeeinstellungen noch nicht geändert. Fehlt die Datei, versucht die Gnome-Shell automatisch, die erkannten Monitore sinnvoll anzuordnen. Da sie im Homeverzeichnis liegt, wird für jeden User eine individuelle Konfiguration gespeichert. Das verhindert aber, dass auch GDM die Datei nutzen kann, da es die monitors.xml mangels Leserechten nicht öffnen kann. Zudem stellt sich bei mehreren Benutzern die Frage, wessen Konfiguration für die Anmeldung gelten soll.

Die Lösung besteht darin, eine monitors.xml mit der gewünschten Konfiguration für GDM an passender Stelle bereitzulegen. Statt sich zu intensiv mit verschachteltem XML-Code herumzuplagen, können Sie die Datei mit den Systemeinstellungen von Gnome erzeugen.

Bevor es losgeht, sichern Sie vorher eine gegebenenfalls vorhandene Konfiguration, indem Sie die Datei an einen anderen Ort verschieben, beispielsweise in die oberste Ebene des Homeverzeichnisses. Im Terminal verwenden Sie dazu folgenden Befehl:

```
mv ~/.config/monitors.xml ~/monitors.original.xml
```

Indem Sie die monitors.xml verschieben und nicht kopieren, befreien Sie zugleich die Konfiguration von eventuellen Altlasten. Denn Gnome überschreibt die Datei nicht plump mit neuen Werten, sondern ergänzt sie mit zusätzlichen, alternativen Einträgen. Das passiert immer dann, wenn sich die Anzahl der angeschlossenen Anzeigegeräte ändert. Durch die mehrfachen Einträge in der XML-Datei erkennt Gnome von Ihnen konfigurierte Setups wieder. Das erspart Ihnen, ständig die Anordnung der Displays neu festzulegen, wenn Sie zwischen Büro und Homeoffice wechseln oder gelegentlich den Fernseher im Wohnzimmer anstöpseln. Doch dieses praktische „Gedächtnis“ neigt dazu, die Konfigurationsdatei aufzublähen. Gibt man diese an GDM weiter, ignoriert es manchmal die Vorgaben oder sucht sich aus der Datei einen anderen Abschnitt aus als den von Ihnen bevorzugten. Wenn Sie die Datei verschieben, beugen Sie dem vor, da Gnome eine neue Datei mit sauberer Konfiguration erzeugt.

Öffnen Sie dazu die Systemeinstellungen, indem Sie auf den Desktophintergrund rechtsklicken und im Kontextmenü „Anzeigeeinstellungen“ wählen. Unter „Bildschirme“ (Ubuntu: „Anzeigegeräte“) ordnen Sie die Monitore so an, wie Sie es für den Anmeldebildschirm später wünschen, und bestätigen Sie mit „Anwenden“. Falls die Anordnung schon passt, ändern Sie irgendwas, bestätigen mit „Anwenden“, ändern es wieder zurück und drücken nochmals „Anwenden“. So erzwingen Sie, dass Gnome die Datei generiert.

Konfiguration platzieren

Nun gilt es, die frisch gebackene XML-Datei für GDM bereitzulegen. Auch GDM schaut unter .config/monitors.xml nach, aber im Homeverzeichnis des Systembenutzers gdm. Je nach Linux-Distribu-

tion befindet sich dieses in /var/lib/gdm oder /var/lib/gdm3. Wo es auf Ihrem System ist, braucht Sie aber nicht zu kümmern, denn ~gdm verweist an die richtige Stelle. Öffnen Sie ein Terminalfenster, kopieren Sie diese Datei in das GDM-Benutzerverzeichnis und passen Sie anschließend die Dateirechte an. Weil Sie dazu Admin-Rechte benötigen, stellen Sie dem Befehl ein sudo voran:

```
sudo cp .config/monitors.xml ~gdm/.config/
monitors.xml

sudo chown gdm:gdm ~gdm/.config/monitors.xml
```

Damit GDM die Konfiguration anwendet, müssen Sie den Dienst neu starten. Dazu wechseln Sie auf eine Textkonsole (zum Beispiel mit Strg+Alt+F4 oder Strg+Alt+F5), melden sich dort mit Benutzername und Passwort an und geben den Befehl `sudo systemctl restart gdm` ein. Meist flackert der Monitor kurz und das System wechselt dann zur von GDM genutzten Konsole, die Sie sonst in der Regel über die Tastenkombination Strg+Alt+F1 erreichen (manchmal auch Strg+Alt+F7). Nun sollte GDM die Monitore so wie von Ihnen konfiguriert einbinden.

Falls in Ihrer anfangs gesicherten monitors.xml-Datei viele liebgewonnene Monitoranordnungen hinterlegt sind, kopieren Sie diese am Ende wieder zurück nach ~/.config, damit Gnome wieder darauf zurückgreifen kann.

Fehlersuche

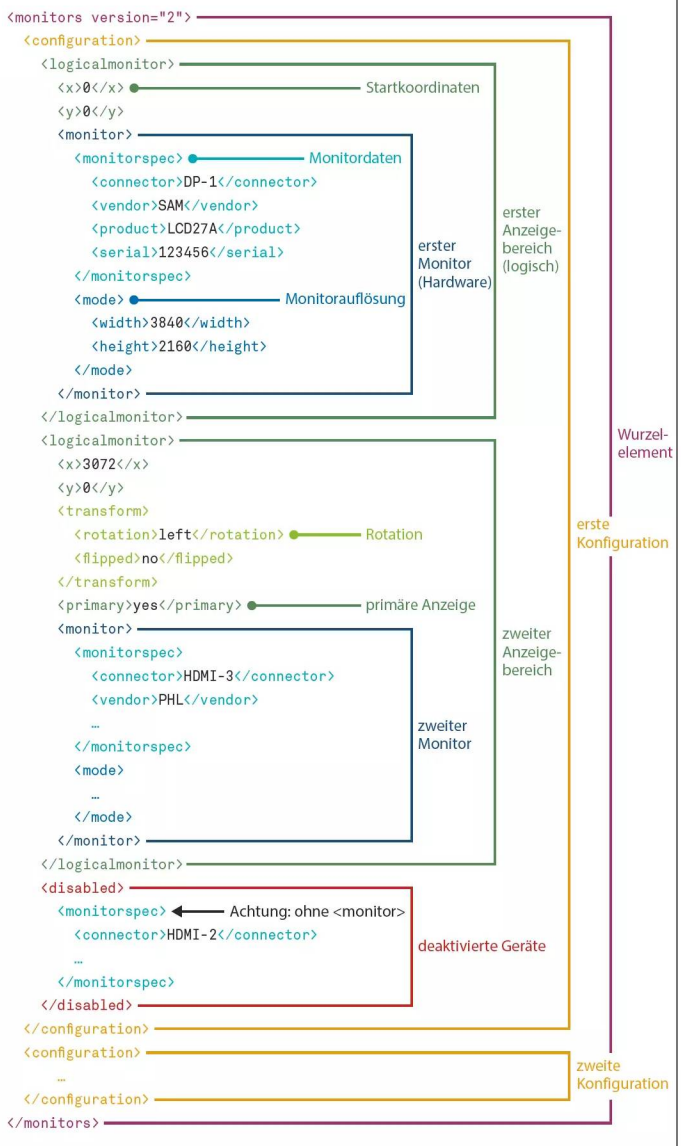
Wenn es nicht klappt, liegt es häufig an einer von zwei Ursachen. Die erste ist eine überladene oder fehlerhafte Konfiguration. Öffnen Sie die von GDM genutzte XML-Datei in einem Texteditor und stellen Sie sicher, dass es mit `<configuration>`nur einen Abschnitt gibt und dieser zu Ihren angeschlossenen Anzeigegeräten passt. Die XML-Struktur erklärt die Infografik rechts.

Damit GDM in der XML-Datei eine Konfiguration wiedererkennt und verwendet, muss innerhalb von `<configuration>` für jedes angeschlossene Gerät ein eigener `<monitorspec>`-Eintrag vorhanden sein, entweder unter `<monitor>` oder `<disabled>`. Gleichzeitig darf es keine Einträge für weitere, nicht angeschlossene Geräte geben. Findet GDM in der Datei keine passende Konfiguration, fällt es auf die Automatik zurück.

Ein anderer typischer Stolperstein besteht darin, dass GDM die Bezeichnungen der Monitoranschlüs-

Der Aufbau der monitors.xml-Datei

Die Datei monitors.xml liefert der Gnome-Shell und GDM Informationen darüber, wie sie erkannte Monitore einbinden sollen. Das Wurzelelement `<monitors>` (Plural) hat eines oder mehrere Elemente vom Typ `<configuration>`. Diese enthalten für eine Gruppe von angeschlossenen Ausgabegeräten die Voreinstellungen. Dabei steht `<monitor>` (Singular) für das konkrete Gerät und enthält Angaben zu Modell, Hersteller und Anschlüssen (`<monitorspec>`) sowie Auflösung (`<mode>`). Der `<logicalmonitor>` beschreibt einen Anzeigebereich (Größe, Position, Skalierung und Drehung), dem mindestens ein Monitor zugeordnet ist. Der primäre Anzeigebereich wird mit `<primary>yes</primary>` festgelegt. Erkannte, aber nicht verwendete Geräte sind unter `<disabled>` mit `<monitorspec>` hinterlegt, aber ohne von `<monitor>` umschlossen zu sein.



se nicht erkennt. Das passiert, wenn die Gnome-Session im X-Server läuft, aber GDM wie auf den meisten aktuellen Linux-Systemen den modernen Wayland-Modus verwendet – oder umgekehrt. Dann steht etwa in der von Gnome erzeugten Konfiguration (`<connector>HDMI-1-2</connector>`), der Monitor sei über „HDMI-1-2“ angeschlossen, aber GDM sieht denselben Anschluss als „HDMI-2“ und findet keine passende Voreinstellung in der monitors.xml.

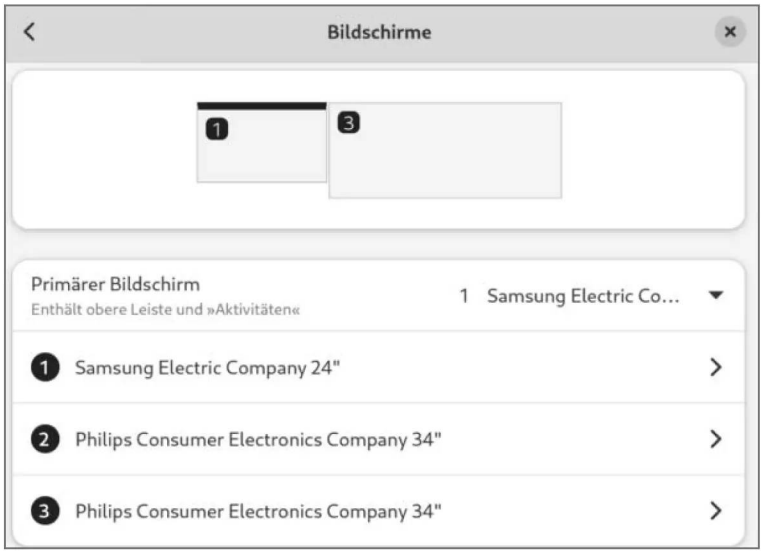
Am einfachsten ist es zu prüfen, welchen Modus Gnome verwendet, und zumindest temporär mit der Gnome-Sitzung den anderen zu verwenden, um eine Konfigurationsdatei mit den passenden Werten zu erzeugen. Einmal eingerichtet, können Sie Ihre Desktopsitzung in dem von Ihnen bevorzugten Modus verwenden, da GDM und Gnome unabhängig voneinander agieren.

Melden Sie sich wie gewohnt in Gnome an und kontrollieren Sie zunächst, welchen Grafikmodus Ihre Desktopumgebung verwendet. Am einfachsten geht das im Terminal durch Eingabe von:

```
echo $XDG_SESSION_TYPE
```

Als Antwort erhalten Sie entweder „wayland“ oder „x11“. Melden Sie sich wieder ab und wählen Sie in der GDM-Anmeldemaske Ihren Benutzernamen aus, ohne aber das Passwort einzugeben. Klicken Sie unten rechts auf das Zahnrad und wählen Sie den benötigten Modus aus. Lautete der Rückgabewert „wayland“, müssen Sie also „Gnome unter Xorg“ oder „Ubuntu auf Xorg“ auswählen. Meldet die Kommandozeile „x11“ als Rückgabewert, gehen Sie entsprechend umgekehrt vor und wählen „Gnome“ oder „Ubuntu“ ohne weitere Zusätze. Verwirrend: Gibt es keine Einträge mit „... Xorg“, aber stattdessen „Ubuntu mit Wayland“, dann starten „Gnome“ oder „Ubuntu“ die Xorg-Sitzung. Geben Sie anschließend Ihr Passwort ein und melden Sie sich an. Prüfen Sie nochmal im Terminal den Session-Typ.

Erzeugen Sie dann wie oben beschrieben eine neue monitors.xml-Datei und kopieren Sie diese ins Verzeichnis ~gdm/.config/. Starten Sie nun GDM erneut, damit der Dienst die neue Konfiguration lädt. Achten Sie darauf, bei Gnome oder Ubuntu wieder den ursprünglichen Modus (Xorg oder Wayland) auszuwählen, wenn alles eingerichtet ist. GDM merkt sich



Mit den Gnome-Anzeigeeinstellungen erzeugen Sie bequem eine Konfigurationsdatei mit Vorgabewerten für GDM.

für jeden Benutzer, welcher Modus als letztes genutzt wurde und verwendet diesen als Vorgabewert.

Hilfsmittel

Bei der Fehlersuche hilft es, die unterschiedlichen XML-Dateien zu vergleichen. Dafür eignet sich das grafische Diff-Werkzeug „Meld“, das Unterschiede zwischen zwei oder drei Dateien farblich hervorhebt. Sie können Meld über die Softwareverwaltung Ihrer Distribution oder aus Flathub nachinstallieren. Gnome sichert bei jeder Änderung der Anzeigeeinstellungen die vorherige Konfiguration in der versteckten Datei ~/.config/monitors.xml~ – die angehängte Tilde gilt auf Linux-Systemen als Konvention für Backup-Dateien. Sichern Sie die von Ihnen selbst erzeugten Konfigurationen, indem Sie diese kopieren und mit selbsterklärenden Namen wie monitors.gespiegelt.xml oder monitors.4K-links-FHD-rechts.xml abspeichern. Öffnen Sie diese Dateien dann mit Meld, um die Unterschiede zu vergleichen.

Da Sie Root-Rechte benötigen, um Dateien im Homeverzeichnis von GDM zu lesen, verwenden Sie in diesem Fall den Kommandozeilenbefehl `diff` im Terminal:

```
sudo diff --color -u ~/.config/monitors.xml↴
                    ↳~gdm/.config/monitors.xml
```

Haben Sie eine funktionierende Konfiguration für ein erstes Setup (zum Beispiel das Homeoffice), können Sie die Schritte ab der Stelle, wo Sie die Konfiguration mithilfe der Gnome-Einstellungen generieren, wiederholen. Oder Sie bauen von Hand weitere `<configuration>`-Abschnitte in die XML-Datei ein und nähern sich so schrittweise der Wunschkonfiguration an. Öffnen Sie dazu mit einem Texteditor die mit Gnome erzeugten monitors.xml-Dateien und kopieren Sie den gewünschten `<configuration>` Abschnitt mit heraus. Fügen Sie dann diesen Block in Ihre für GDM bestimmte monitors.xml ein, und zwar unterhalb von `<monitors>` .

Achten Sie darauf, dass es nur einen einzigen `<configuration>`-Block für jede Kombination von Ausgabegeräten gibt. Entscheidend sind dafür die Einträge mit `<monitorspec>`.

Schlussstrich

Dieser ganze Aufwand wäre nicht nötig, würden die GDM-Entwickler wie bei anderen Displaymanagern den Anmeldebildschirm einfach auf allen Monitoren spiegeln. Zumindest bietet das XML-Gebastel eine Möglichkeit, doch auf die Anzeige des Anmeldebildschirms Einfluss zu nehmen.

Vorsicht: In manchen Onlineforen gibt es den Tipp, per Skript oder Systemd-Aufruf die monitors.xml automatisch aus dem eigenen Home-Verzeichnis ins GDM-Verzeichnis zu kopieren. Das klingt zunächst bequem, birgt aber auch die Gefahr, versehentlich eine funktionierende Konfiguration zu zerschießen. Das Frustpotenzial ist deutlich höher als der Nutzen. (ktn) **c't**

GDM-Bugreport und Beispielkonfiguration zum Download

ct.de/wbcz

// heise devSec()

Die Konferenz für sichere Software- und Webentwicklung

11.–13. September 2023 in Karlsruhe

Sichere Software beginnt vor der ersten Zeile Code

Security ist fester Bestandteil der Softwareentwicklung – vom **Entwurf** über den **Entwicklungsprozess** bis zum **Deployment.**

Die **heise devSec** hilft Ihnen dabei mit Vorträgen zu den wichtigsten Themen wie Software Supply Chain, Kryptografie und der Auswirkung von KI auf die Sicherheit.

Aus dem Programm:

// Das ABC sicherer Webanwendungen
// Software Supply Chain Security mit dem SLSA
// Multifaktor-Authentifizierung in der Praxis
// Skalierung von Sicherheit in Kubernetes
// Erweiterung des Secure Development Lifecycle um Privacy by Design
// Wie man mit Mathematik eine Bank übernehmen kann

JETZT **TICKETS** SICHERN!

www.heise-devsec.de

Workshops am 11. September
OAuth 2.1 und OpenID Connect | DevOps und der API-Lebenszyklus | Legacy-Software

Veranstalter

iX Magazin für professionelle IT
dpunkt.verlag
heise Security

Gold-Sponsoren

Contrast Security
opentext | Cybersecurity
ROHDE&SCHWARZ Make ideas real
sysdig
WIBU SYSTEMS

Bronze-Sponsor

andrena objects

Gnome für große Monitore einrichten

Wer einen übergroßen Monitor nutzen will, stößt mit den Voreinstellungen von Gnome schnell an Grenzen. Wir zeigen, welche Einstellungen und Erweiterungen auch Pixelmonster optimal bespielen.

Von **Keywan Tonekaboni**

Der neue Monitor für den Linux-Rechner ist da! Endlich genug Fläche für all die vielen Fenster. Doch mehr Pixel allein lösen nicht alle Probleme und schaffen neue, denn Gnome hilft kaum dabei, Fenster effizient auf einer großen Bildschirmfläche zu verteilen. Zwar gibt es eine Einrasthilfe, die Fenstergrößen automatisch anpasst. Doch während Windows oder KDE Plasma das Fenster auch auf ein Viertel der Displayfläche reduzieren, kann Gnome sie nur auf eine der beiden Hälften schieben.

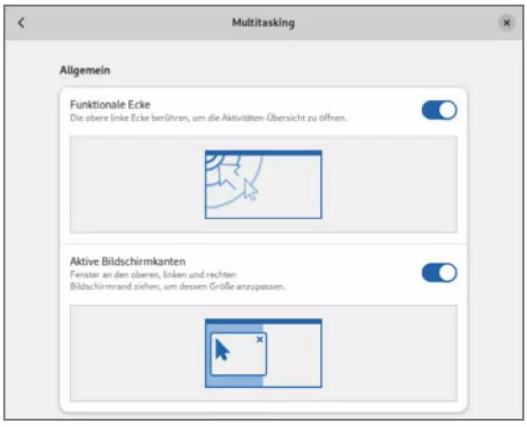
Mit den richtigen Hilfsmitteln glänzt der Gnome-Desktop auch auf der großen Bildschirmfläche. Allerdings schießen in manchen Situationen Tools quer, die sonst gute Dienste leisten. Wir stellen daher sinnvolle Einstellungen und praktische Erweiterungen vor für übergroße oder überbreite Monitore.

Optimieren ohne Tweaks

Seit Gnome-Version 41 enthält „Einstellungen“ den Abschnitt „Multitasking“, der eine Handvoll Optionen listet, die das Verhalten der Gnome-Bedienoberfläche beeinflussen. Die meisten davon gibt es seit Einführung der Gnome-Shell, nur waren sie bislang versteckt. Ändern ließen sich diese Optionen unter anderem über das Zusatzprogramm „Gnome Optimierungen“. Das besser als Tweak-Tool bekannte Werkzeug ist jetzt weitgehend überflüssig.

Falls abgeschaltet, können Sie unter „Multitasking“ die aktiven Bildschirmkanten einschalten, worauf sich die Größe eines Fensters anpasst, wenn Sie es an den Bildschirmrand ziehen. So eine Funktion heißt auf Englisch „Tiling“ oder „Snap Layout“. Die Gnome-Einrasthilfe kann Fenster nur auf die rechte beziehungsweise linke Hälfte des Bildschirms zwingen oder sie auf die gesamte Displayfläche maximieren. Später im Text stellen wir Erweiterungen vor, die ein flexibleres und ausgefeilteres Tiling erlauben. Solche Erweiterungen deaktiviert die Funktion der aktiven Bildschirmkanten von Gnome, um Wechselwirkungen damit zu vermeiden.

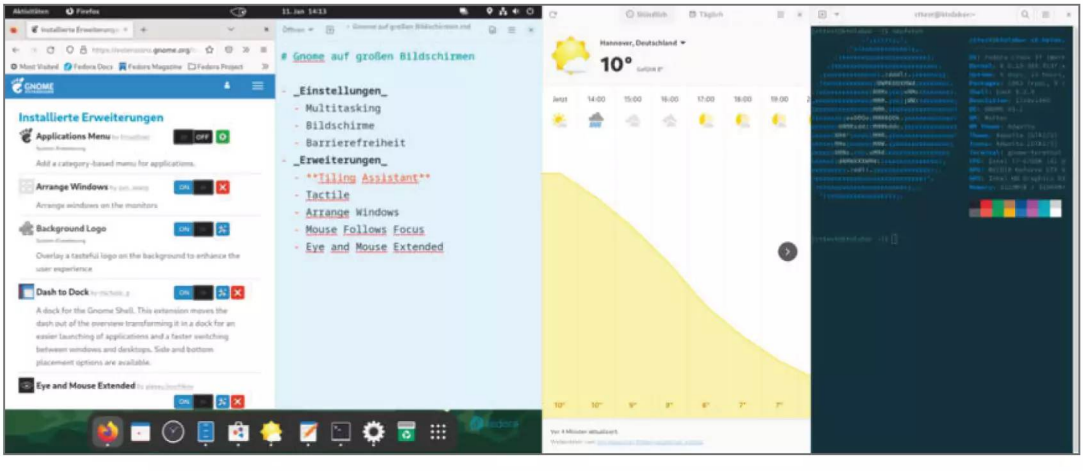
Ab Werk besitzt Gnome außer dem sichtbaren Desktop noch weitere virtuelle Arbeitsflächen, zwischen denen Sie über die Aktivitätenübersicht oder mit Tastenkombination Super+Alt+Pfeiltaste links/rechts wechseln. Verwenden Sie mehrere Monitore, dann richtet Gnome normalerweise die virtuellen Arbeitsflächen nur für den primären Bildschirm ein.



Das Verhalten des Gnome-Desktops ändern Sie in den Einstellungen unter Multitasking, etwa um Fenster am Bildschirmrand einschnappen zu lassen.

Das ist der Monitor, der auch die Menüleiste und das Dock anzeigt. Unter „Multitasking“ können Sie bei der Nutzung mehrerer Monitore Gnome anweisen, auf allen Bildschirmen virtuelle Arbeitsflächen einzurichten.

Der Vorteil der Gnome-Vorgabe: Auf dem zweiten Monitor mit statischer Arbeitsfläche platziert man Fenster, die man stets im Blick haben möchte, wie ein Mailprogramm, Chatfenster oder Systemanzeigen. Tauscht man beispielsweise zwei 16:9-Bildschir-



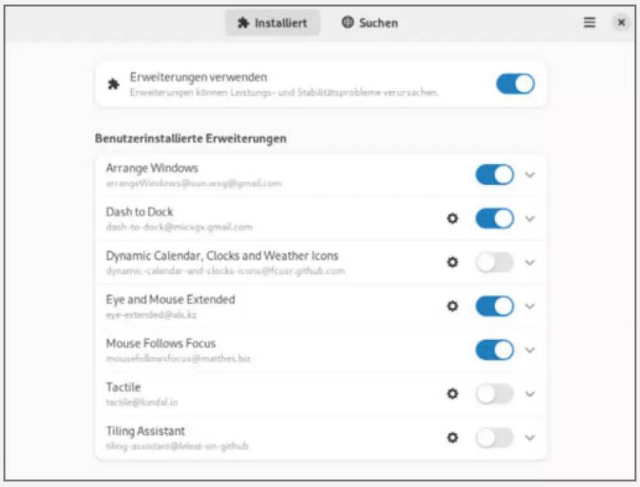
Beherrscht Ihr überbreiter Bildschirm den Picture-by-Picture-Modus, trotzen Sie Gnome ein vierspaltiges Tiling ab, wenn Sie Ihren Monitor mit zwei Kabeln parallel anschließen.

Shell-Erweiterungen installieren

Am einfachsten installieren Sie Gnome-Shell-Erweiterungen mit dem „Erweiterungs-Manager“ (Extension Manager), den Sie via Flathub beziehen. Diese App sucht im Extension-Repository des Gnome-Projektes nach Erweiterungen und bietet an, diese zu installieren und zu verwalten. Einziges Manko: Nachdem Sie eine Erweiterung installiert haben, müssen Sie von der Suche wieder zum Tab „Installiert“ wechseln, um sie zu verwalten.

Alternativ installieren Sie Erweiterungen mit dem Webbrowser über die Webseite extensions.gnome.org. Rüsten Sie dazu zunächst über die Paketverwaltung Ihrer Distribution das Paket `chrome-gnome-shell` oder `gnome-browser-connector` sowie im Browser die Erweiterung „GNOME Shell-Integration“ nach[2], was die Webseite von sich aus anbietet.

Die Einstellungen der Erweiterungen öffnen Sie, soweit vorhanden, in der App Erweiterungs-Manager über den Tab „Installiert“ oder im Browser auf der Webseite für Gnome-Erweiterungen im Abschnitt „Installed Extensions“, indem Sie jeweils in der Liste auf das Zahnrad- oder Werkzeug-Icon neben dem Namen der Erweiterung klicken. Es öffnet sich ein separates Fenster mit den Optionen.



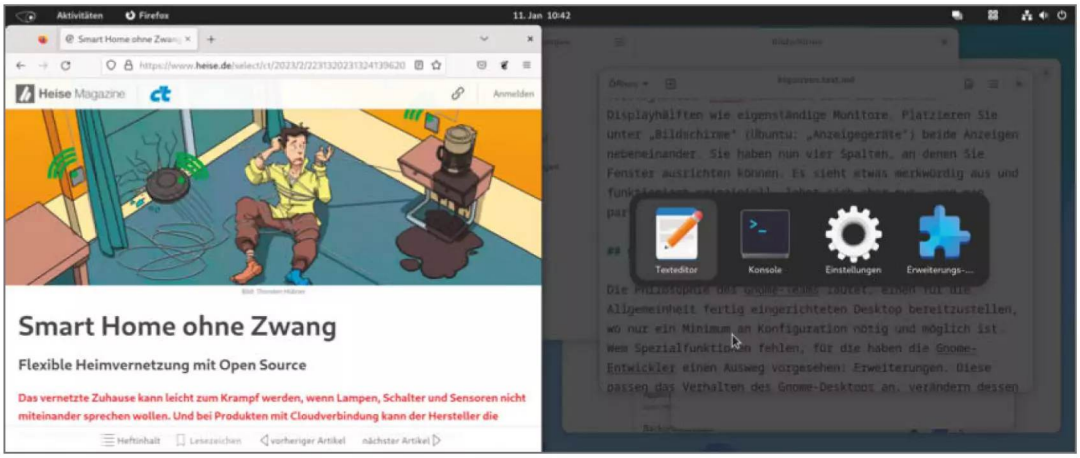
Der unabhängig von Gnome entwickelte Erweiterungs-Manager vereinfacht die Suche, Installation und Verwaltung von Gnome Shell Extensions.

me gegen einen überbreiten 21:9-Monitor, fällt die statische Arbeitsfläche weg. Als Workaround können Sie Fenster, die Sie immer im Blick haben müssen, auf alle Arbeitsflächen pinnen. Klicken Sie dazu mit der rechten Maustaste auf die Titelleiste des gewünschten Programmfensters, beispielsweise der Messenger-App. Wählen Sie im Fenstermenü den Eintrag „Immer auf der sichtbaren Arbeitsfläche“. Dann nimmt Gnome beim Wechsel der Arbeitsfläche das Fenster mit. Bei manchen Programmen wie Microsoft Teams fehlt die Titelleiste. Hier öffnen Sie das Fenstermenü, indem Sie beim Rechtsklick zusätzlich die Super-Taste (Windows-Taste) gedrückt halten.

Mit einem Hack können Sie die Arbeitsflächen-Einstellungen nutzen, um ohne zusätzliche Erweiterungen das Tiling auf extrabreiten Monitoren zu verfeinern. Verfügt Ihr Monitor über mehrere Displayeingänge und unterstützt die Funktion Picture-by-Picture, schließen Sie ihn mit zwei Kabeln an den Computer an. Gnome behandelt die erkannten Displayflächen wie eigenständige Monitore. Platzieren Sie unter „Bildschirme“ (Ubuntu: „Anzeigegeräte“) beide Anzeigen nebeneinander. Dadurch erhalten Sie vier Spalten, an denen Sie Fenster ausrichten können. Es sieht etwas merkwürdig aus und funktioniert prinzipiell, lohnt sich aber nur, wenn man partout keine Erweiterungen installieren möchte.

Gnome-Desktop mit Erweiterungen tunen

Die Philosophie des Gnome-Teams lautet, einen Desktop bereitzustellen, der nur ein Minimum an Konfiguration braucht und ermöglicht. Für Spezialfunktionen haben die Gnome-Entwickler einen Ausweg vorgesehen: Erweiterungen. Diese passen das Verhalten des Gnome-Desktops an, verändern sein Layout und fügen neue Funktionen hinzu oder integrieren jene anderer Anwendungen in die Bedien-



Die Erweiterung Tiling Assistant baut die Einrastfunktion aus. Sie gruppiert die Fenster, woraufhin Sie diese gemeinsam in den Vordergrund heben oder deren Größen simultan ändern können.

oberfläche. Dazu modifizieren Erweiterungen den Programmcode der Gnome-Shell, was Einfluss auf die Stabilität des Desktops haben kann. Deshalb kann es auch vorkommen, dass sich Extensions gegenseitig in die Quere kommen.

Daher ein Wort der Warnung: Erweiterungen sind dafür gedacht, den Gnome-Desktop punktuell anzupassen, nicht dazu, das ganze Bedienkonzept auf den Kopf zu stellen. Verwenden Sie daher nur benötigte Erweiterungen oder greifen Sie gleich zu einer anderen Desktopumgebung. Deinstallieren Sie außerdem nicht benötigte Erweiterungen, da diese auch im deaktivierten Zustand beim Start der Gnome-Shell initialisiert werden. Wer diese Hinweise beachtet, kann mit einer Handvoll Erweiterungen viel Spaß haben.

Teilen und herrschen

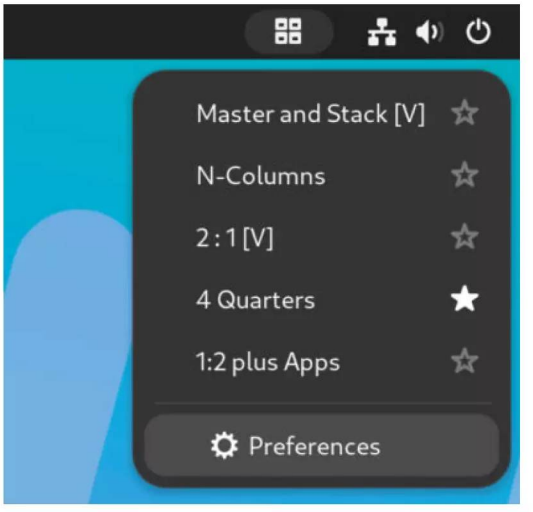
Mitunter die erste Frage, die sich bei übergroßen und extrabreiten Bildschirmflächen stellt: Wie platziere ich die Fenster möglichst effizient? Auf einem 21:9-Display will man selten Fenster auf die ganze Fläche maximieren. Hier kommt das Tiling ins Spiel, also das Einrasten und Unterteilen der Fenster anhand eines festen Rasters – zum Beispiel vier Viertel – oder nach einem Muster zu teilen, etwa die Fläche dynamisch durch die Anzahl der geöffneten Fenster. Interessanterweise greift das Tiling teils auf Konzepte von sehr nerdigen Bedienoberflächen zurück, wie den Tiling-Window-Managern [1]. Zahlreiche Erweiterungen ersetzen oder ergänzen die Tiling-Funktion von Gnome.

Eine sehr flexible und umfangreiche Erweiterung ist der „Tiling Assistant“, der trotzdem relativ intuitiv zu bedienen ist. Ubuntu arbeitet derzeit daran den Tiling Assistant in seinen Desktop einzubauen. Den Eintrag zu dieser Erweiterung auf extensions.gnome.org (siehe Kasten „Shell-Erweiterungen installieren“) und die für alle weiteren Extensions haben wir für Sie unter ct.de/wfut verlinkt. Der Tiling Assistant ändert zunächst zwei Dinge: Wenn Sie ein Fenster an den Rand ziehen, gibt es zusätzliche Optionen, wie das Fenster einrasten kann, beispielsweise in der oberen Bildschirmhälfte oder in einer Ecke. Lassen Sie Fenster in einer dieser Zonen einrasten, öffnet sich ein Pop-up mit Icons aller weiteren geöffneten Programme. Wählt man ein Icon aus, platziert der Tiling Assistant das zugehörige Fenster auf der freien Fläche. Zusätzlich gruppiert es die Fenster. Wird ein Fenster der Gruppe angehoben, also vor andere Fenster gezeichnet, dann hebt der Tiling Assistant alle anderen Fenster mit an. Wechselt man die Arbeitsfläche, visualisiert eine kleine Animation, welches Fenster den Fokus hat.

Verschieben Sie ein Fenster mit der Maus und halten dabei die Strg-Taste gedrückt, dann rastet das Fenster nicht nur im Monitorrand ein, sondern auch bei bereits eingerasteten anderen Fenstern. Beide Fenster teilen sich dann die Fläche. Wenn Sie die Größe des einen Fensters ändern, zieht das andere Fenster mit. Probieren Sie es einfach aus; Tiling As-

sistant zeigt in einer Animation, wo das Fenster einrastet.

Zusätzlich zur Mausbedienung gibt es Tastenkombinationen, um die Fenster zu platzieren. Wie bei der Gnome-Tiling-Funktion verschiebt die Tastenkombination aus Super-Taste und der linken Pfeiltaste das Fenster beispielsweise auf die linke Hälfte. Darüber hinaus kann man die Super-Taste aber auch mit einer Taste des Ziffernblocks kombinieren. Bei Super+9 vom Ziffernblock landet das ausgewählte Fenster in der oberen, rechten Ecke.



Wechseln Sie blitzschnell über das Panelmenü das Raster-Layout, nach dem Tiling Assistant die Fenster anordnet.

Viele dieser Vorgaben können Sie nach Belieben anpassen – etwa das Kachel-Pop-up abschalten oder die Tastenkombinationen verändern. Öffnen Sie dazu in der Erweiterungsverwaltung die Einstellungen des Tiling Assistant. Die meisten Optionen sind selbsterklärend.

Wenn Sie den Gnome-Desktop im Wayland-Modus nutzen, kann es Darstellungsfehler mit der Fokus-Animation geben. Deaktivieren Sie in diesem Fall die Animation unter „Active Window Hint“. Verlieren Sie oft die Übersicht, welches Fenster den Fokus hat, können Sie mit der Einstellung „Always“ den Tiling Assistant anweisen, dauerhaft einen blauen Rand um das fokussierte Fenster zu zeichnen. Auch diese Einstellung kann im Wayland-Modus Probleme verursachen.

Der Abschnitt „Dynamisches Tastenbelegungsverhalten“ verändert das Verhalten von Tastenkombinationen abhängig vom Zustand des geteilten Fensters. Bei „Fester Fokus“ wechseln die Tastenkombinationen das aktiv ausgewählte Fenster, wenn es schon im Raster platziert ist. Ein links eingeschnapptes Fenster springt dann mit Super+6 (vom Ziffernblock) nicht nach rechts, sondern wechselt den Fokus, wenn rechts ein anderes eingerastetes Fenster vorhanden ist. Mit der Auswahl „Kachelzustand“ ändern Tastenkombinationen die Größe des eingerasteten Fensters. Befindet sich das ausgewählte Fenster auf der linken Hälfte und Sie drücken Super+2, wechselt das Fenster in die untere linke Ecke; ohne „Kachelzustand“ würde das Fenster die gesamte untere Hälfte belegen. Wenn Sie diese Beschreibung verwirrt und Sie nicht vorhaben, Fenster mit Tastenkombinationen wild hin und her zu scheuchen, belassen Sie das dynamische Tastenbelegungsverhalten in der Grundeinstellung, also deaktiviert.

Layouts mit Tiling Assistant

Die wohl spannendste Funktion versteckt der Tiling Assistant als experimentelles Feature: Layouts. Damit legen Sie individuelle Raster an, die von der schnöden Vierteilung abweichen und sich optional dynamisch erweitern. Ein Layout könnte etwa rechts zwei kleine Kacheln für Chatfenster vorsehen und links eine große Fläche für den Browser, ein Office-Programm oder die Entwicklungsumgebung. Wenn Sie ein Layout aktivieren, dann bietet Tiling Assistant an, mit dem Kachel-Pop-up alle geöffneten Fenster anhand des Layouts anzuordnen.

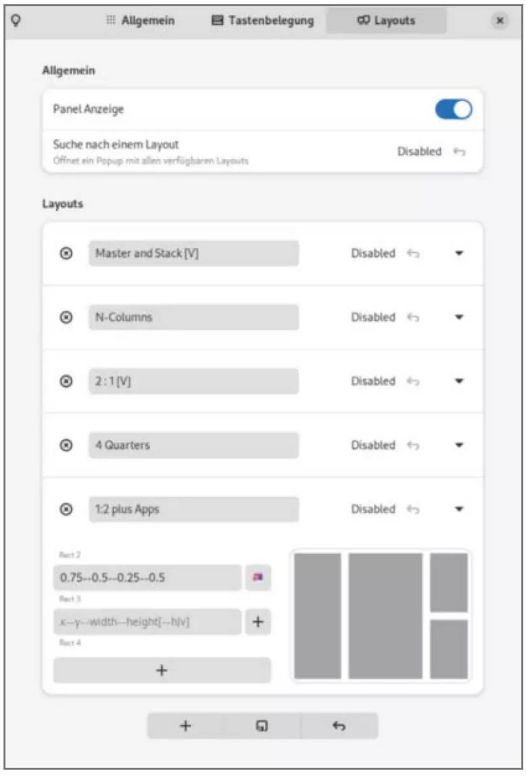
Um die Layout-Funktion freizuschalten, öffnen Sie die Einstellungen des Tiling Assistant und klicken links in der Titelleiste auf die Glühbirne (Ubuntu: Info-Icon). Daraufhin öffnet sich ein Menü. Wählen Sie den Eintrag „Fortgeschrittene …“ aus und aktivieren Sie dort den Schalter „Erweiterte/Experimentelle Einstellungen“. Wenn Sie mit dem Pfeil in der Titelleiste in das Menü „Einstellungen“ zurückkehren, sehen Sie einen neuen Tab namens „Layouts“. Vier Layouts sind in Tiling Assistant bereits definiert: „Master and Stack [V]“, „N-Columns“, „2:1 [V]“ und „4 Quarters“. Das letzte verhält sich wie das Standardlayout mit zwei Spalten und zwei Zeilen.

Bei „Master und Stack [V]“ gibt es ein Hauptfenster auf der linken Bildschirmhälfte. Die andere Hälfte teilt Tiling Assistant horizontal unter den Fenstern auf, die Sie über das Kachel-Pop-up auswählen. Bei vier Fenstern wären diese so aufgeteilt: links eine

Spalte mit einer Zeile und rechts eine Spalte mit drei Zeilen.

Das Layout „N-Columns“, also N-Spalten, teilt die Fläche vertikal anhand der ausgewählten Fenster auf. Die Spaltenbreite entspricht der Bildschirmbreite geteilt durch die Anzahl der ausgewählten Fenster. Während N-Columns dynamisch agiert, verhält sich das Layout „2:1 [V]“ statisch: eine zweidrittel große Kachel links und eine weitere Kachel rechts im dritten Drittel bieten Platz für insgesamt zwei Fenster. Der Zusatz „[V]“ ist ein Hinweis auf die vertikale Aufteilung.

Die Layouts wechseln Sie über ein Panel-Menü, das Sie in den Layout-Einstellungen aktivieren. Alternativ oder zusätzlich können Sie einem Layout eine eigene Tastenkombination zuweisen. Jedes Mal, wenn Sie ein Layout aktivieren, öffnet Tiling Assistant das Kachel-Pop-up, mit dem Sie die geöffneten Programmfenster im Layout anordnen. Sie können ein Layout durch Anklicken des Sternchens im Panel-Menü als Favorit festlegen. Halten Sie anschließend die Alt-Taste gedrückt, wenn Sie ein Fenster verschieben, dann bietet Tiling Assistant an, das Fenster anhand des favorisierten Layouts einzurasten. Halten Sie zusätzlich zu Alt noch die Super-Taste gedrückt, um das Fenster über mehrere Kacheln aufzuziehen.



Passen Sie in den Einstellungen von Tiling Assistant die Layouts an und legen Sie fest, welche Apps automatisch mit dem Layout starten sollen.

Raster-Layouts selbst gemacht

Ein eigenes Layout zu erzeugen ist machbar, aber mangels komfortablem Interface etwas umständlich. Es hilft, wenn Sie ein fertiges Layout als Vorlage verwenden. Klicken Sie zunächst in den Layout-Einstellungen unter der Liste der verfügbaren Layouts auf das Plus-Symbol, um ein neues Layout anzulegen. Vergeben Sie dann einen Namen, der idealerweise dem Layoutkonzept entspricht („6 Sechstel“ statt „Mein Layout“). So müssen Sie später nicht grübeln, welches das gesuchte Layout ist.

Die erste Kachel definieren Sie mit dem Textfeld „Rect 0“ unterhalb des Namens, wobei Sie Größe und Position als Zeichenkette eintragen. Die Syntax setzt sich aus der Position auf der X-Achse und Y-Achse sowie der Breite und Höhe der Kachel zusammen, jeweils getrennt durch zwei Bindestriche: `x--y--Breite--Höhe`, wobei Breite die Kachel nach rechts zeichnet und Höhe nach unten. So definiert `0--0.5--0.33--0.5` eine Kachel in der unteren linken Ecke, die ein Drittel der Bildschirmbreite breit und die Hälfte der Bildschirmhöhe hoch ist. Die Werte sind Dezimalbrüche, also 0.5 für die Hälfte, 1.0 für die ganze Breite beziehungsweise Höhe, relativ zur Monitorgröße. Der Koordinatenursprung (x=0, y=0) befindet sich in der oberen linken Bildschirmecke. Mit der großen Plus-Schaltfläche unter dem Textfeld fügen Sie zusätzliche Textfelder hinzu, mit dem Sie die weiteren Kacheln definieren.

Für ein Layout mit sechs Sechsteln sehen die Angaben dann so aus:

```
Rect 0: 0--0--0.33--0.5

Rect 1: 0--0.5--0.33--0.5

Rect 2: 0.33--0--0.33--0.5

Rect 3: 0.33--0.5--0.33--0.5

Rect 4: 0.66--0--0.33--0.5

Rect 5: 0.66--0.5--0.33--0.5
```

Die Kacheln dürfen sich nicht überlappen. Sie können, müssen aber nicht die ganze Fläche dem Layout zuteilen. Eine Grafik visualisiert die Aufteilung der

Fläche und warnt bei Syntaxfehlern oder überlappenden Kacheln. Speichern Sie die Layoutdefinitionen über den Speichern-Knopf unterhalb der Liste.

Damit eine Fläche wie bei N-Columns dynamisch auf die ausgewählten Fenster verteilt wird, ergänzen Sie am Ende `--v` für eine vertikale oder `--h` für eine horizontale Aufteilung. So definiert `0.5--0--0.5--1--h` eine Kachel in der rechten Hälfte, worin alle zugewiesenen Fenster übereinander gestapelt werden, also die Fläche unter ihnen horizontal aufgeteilt ist.

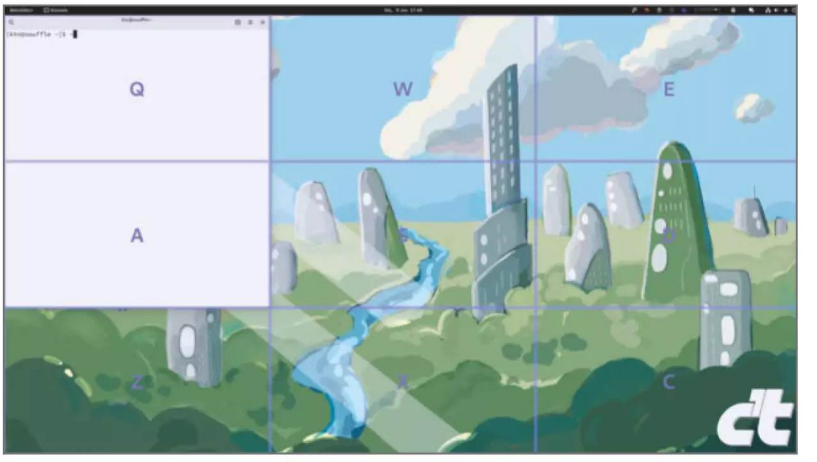
Rechts neben den Textfeldern gibt es je Zeile eine weitere Schaltfläche mit einem Plussymbol. Hier können Sie der Kachel eine Anwendung zuweisen, die Tiling Assistant startet, sobald Sie das Layout aktivieren. Möchten Sie das Layout über eine Tastenkombination aktivieren, weisen Sie diese über die Schaltfläche („Disabled“) neben dem Layoutnamen zu.

Im GitHub-Repository von Tiling Assistant finden Sie eine umfangreiche englischsprachige Dokumentation zu dynamischen Tastenkürzeln, verschiedenen Tiling-Modi und Layouts. Sie erreichen diese über die Info-Schaltfläche im Einstellungsfenster. Wählen Sie im Menü das Benutzerhandbuch aus.

Neben Tiling Assistant gibt es unter den Gnome-Erweiterungen weitere Extensions, die die Anordnung der Fenster erleichtern – beispielsweise gTile, gSnap oder Material Shell. Falls Ihnen das Prinzip gefällt, aber Tiling Assistant nicht zusagt, probieren Sie eine der genannten anderen Erweiterungen aus. Aktivieren Sie besser nicht mehrere Tiling-Erweiterungen gleichzeitig, um Wechselwirkungen zwischen ihnen zu vermeiden.

Raster mit Tactile

Wenn Sie nur die Fenster per Tastenkombination an einem simplen Raster ausrichten wollen, ist die Erweiterung „Tactile“ eine bescheidene Alternative. Mit Super+T blenden Sie ein Raster ein, beispielsweise 4 × 2 Felder, die jeweils mit einem Buchstaben beschriftet sind. Um das fokussierte Fenster auf dem Raster zu positionieren, drücken Sie zwei der angezeigten Buchstaben. Daraufhin zieht Tactile das Fenster zwischen beiden Feldern auf. Da die angezeigten Buchstaben passend zur Tastaturbelegung verteilt sind – zum Beispiel Q, W, E, R und A, S, D, F – klappt das flott und intuitiv. Die Tastenfolge Super+T, Q, A zieht das Fenster von der oberen linken Ecke bis zur unteren linken Ecke auf, wobei es nur ein Viertel der Bildschirmbreite einnimmt. Wollen Sie das Fenster auf nur ein Feld verkleinern, drücken sie zweimal den gleichen Buchstaben (Super+T, Q, Q).



Die Erweiterung „Tactile“ blendet ein Raster ein, um darin Fenster zu platzieren. Dazu reicht es für die gewünschten Kacheln die angezeigten Buchstaben zu drücken.

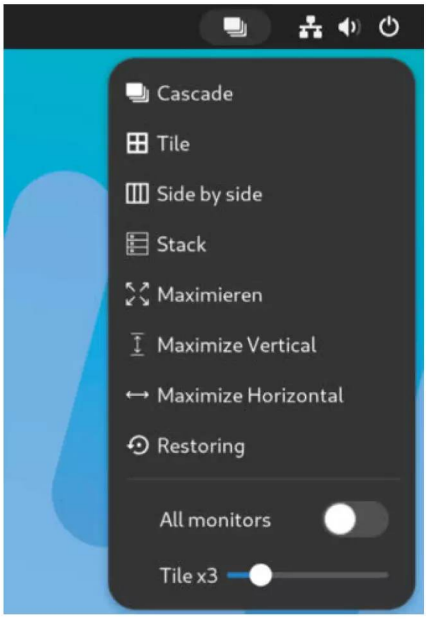
In Tactile stehen für das Raster bis zu vier Layouts zur Verfügung. Drücken Sie nach Super-T eine Ziffer zwischen 1 und 4, wechselt das Raster zur jeweiligen Vorlage. Die Layouts können Sie in den Einstellungen der Erweiterung ändern. Sie lassen sich viel einfacher anpassen als bei Tiling Assistant, dafür sind sie weniger flexibel. Tactile arbeitet mit vier Spalten und drei Zeilen. Deren Größenverhältnis bestimmen Sie, indem Sie diesen jeweils eine Ganzzahl größer oder gleich Null zuweisen. Mit dem Wert gewichten Sie die Breite der Spalte beziehungsweise die Höhe der Zeile. Eine Spalte mit dem Wert 2 ist doppelt so breit wie eine mit dem Wert 1. Bei 0 blendet Tactile die Zeile oder Spalte aus. Die konkrete Spaltenbreite oder Zeilenhöhe ergibt sich aus der Gesamtfläche geteilt durch die Summe der vergebenen Gewichte und multipliziert mit dem Wert für die Spalte oder Zeile.

Fenster automatisch arrangieren

Wenn Ihnen gar nicht danach ist, die Fenster händisch zu verteilen, assistiert Ihnen die Erweiterung „Arrange Windows“. Sie platziert alle geöffneten Fenster einer Arbeitsfläche nach einem vorgegebenen Muster, etwa alle nebeneinander als Spalten. Nach der Installation von Arrange Windows finden Sie rechts oben im Panel ein neues Icon, das einem Kartenstapel ähnelt. Ein Klick darauf öffnet ein Menü. Darüber bestimmen Sie, wie Arrange Windows die geöffneten Programmfenster, nun ja, arrangiert. Zur

Auswahl stehen: Cascade (Fenster übereinander mit leichtem Versatz), Tile (Raster), Side by Side (als Spalten nebeneinander), Stack (als Zeilen übereinander), sowie Maximieren, wahlweise auch nur in der Höhe (Maximize Vertical) oder Breite (Maximize Horizontal).

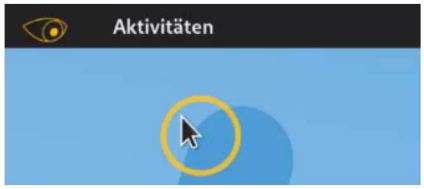
Die Aktion wendet Arrange Windows immer auf alle Fenster der sichtbaren Arbeitsfläche simultan an. „Restoring“ soll die ursprünglichen Positionen und Ausmaße der Fenster wiederherstellen, allerdings unzuverlässig. Für die ersten vier Aktionen – Cascade, Tile, Side by Side und Stack – gibt es auch Tastenkombinationen (Strg+Alt+1…4).



Wenn Sie viele Fenster blitzschnell umsortieren möchten, leistet die Erweiterung „Arrange Windows“ gute Dienste.

Maus-Cursor aufstöbern

Übergroße Monitore werfen nicht nur die Frage auf, wie man die Fenster am besten organisiert. Suchen Sie manchmal auf den unendlichen Weiten des Bildschirms nach dem Mauszeiger? Dann hilft eine Option aus den Gnome-Einstellungen. Aktivieren Sie im Abschnitt Barrierefreiheit unter „Zeigen und Klicken“ die Einstellung „Mauszeiger finden“. Wenn Sie die Strg-Taste drücken, hebt eine kreisförmige Animation die Position des Mauszeigers hervor. Unter Barrierefreiheit können Sie auch die Größe des Mauszeigers ändern.



Wie Saurons Auge verfolgt die Erweiterung „Eye and Mouse Extended“ den Mauszeiger auf Schritt und Tritt und hebt diesen auf Wunsch auch farblich hervor.

Die Erweiterung „Eye and Mouse Extended“ löst die Sichtbarkeit des Mauszeigers auf eine Weise, die langjährigen Linux-Usern vertraut vorkommen dürfte: Es platziert im Panel ein Auge, das ununterbrochen auf den Mauszeiger blickt. Wollen Sie wissen, wo der Mauscursor steckt, müssen Sie nur dem Blick des Panel-Auges folgen. Klicken Sie auf das Auge, zeichnet die Erweiterung dauerhaft einen farbigen Kreis um den Mauszeiger und steigert so dessen Sichtbarkeit. Die Position des Auges im Panel und die Farbe sowie das Erscheinungsbild der Mauszeigermarkierung ändern Sie in den Einstellungen.

Falls Sie oft per Tastenkürzel zwischen Programmen wechseln und Ihnen die langen Mauswege zum ausgewählten Fenster lästig sind, verkürzt die Erweiterung „Mouse Follows Focus“ die Strecke. Die Extension „beamt“ den Mauszeiger stets in die Mitte des Fensters, das den Fokus hat. Die Funktion ist gewöhnungsbedürftig, da der Mauszeiger auch unerwartet wegspringen kann, wenn sich plötzlich irgendwo ein neues Fenster öffnet. Probieren Sie aus, ob die Erweiterung Ihnen Arbeit abnimmt oder zusätzlichen Kummer bereitet.

Weniger ist mehr

Die Suche mit Begriffen wie „Snap“ oder „Tiling“ im Erweiterungskatalog bringt weitere praktische Extensions hervor. Die leistungsfähigste Erweiterung auf großen Bildschirmen bleibt wohl der Tiling Assistant, wobei es die praktische Layout-Funktion vor unbedarften Nutzern verbirgt. Aber auch Tactile und Arrange Windows helfen, Fenster schnell auf der Bildschirmfläche zu platzieren.

Achten Sie bei Erweiterungen auf die Kommentare und Bewertungen im Katalog und prüfen Sie auf der jeweiligen Projekt-Homepage (meist ein GitHub-Repository), ob die Erweiterung gepflegt wird. Auch wenn Sie auf dem großen Bildschirm nicht so asketisch agieren wollen, wie es das Gnome-Projekt vorgibt, sollten Sie es mit den Zusatzfunktionen nicht übertreiben. Am effizientesten bleibt am Ende ein stabiler Desktop. (ktn) c't

Literatur

[1] Anna Simon, Dynamisches Raster, Awesome: effizienter Unix-Desktop nach Maß, c't 15/2020, S. 152

[2] Keywan Tonekaboni, Desktop-Modding, Gnome- und Ubuntu-Desktop durch Erweiterungen individuell anpassen, c't 4/2020, S. 152

Links zu Erweiterungen und Extension-Webseite

ct.de/wfut

Bild: Albert Hulm

Performance-Overlay für Spiele & mehr

Das Steam Deck hat es vorgemacht und ein praktisches Game-Overlay fest in seine Steam-Oberfläche eingebaut, das die Hardware-Auslastung anzeigt. Mit wenigen Handgriffen ist das Vulkan- und OpenGL-Overlay mit MangoHud aber auch auf jedem Linux-Desktop eingerichtet.

Von **Liane M. Dubowy**

Spiel starten und loslegen: Wer in virtuelle Welten eintauchen und abschalten will, ist genervt, wenn's ruckelt und hakt. Nun gilt es, den Spielverderber schnell zu finden. Ob der Prozessor voll ausgelastet, die Grafikkarte zu heiß oder der Arbeitsspeicher voll ist, verrät MangoHud via Overlay, das sich auf dem Bildschirm als Einblendung über das laufende Programm legt. Bei Bedarf schreibt es die Daten zur späteren Analyse in eine Tabelle, sodass sie Sie später analysieren und vergleichen können. Wer Valves Handheld-Konsole Steam Deck besitzt, kennt das hilfreiche Overlay bereits, denn dort ist ab Werk das Tool MangoApp desselben Entwicklers vorkonfiguriert.

Doch auch bei ressourcenfordernden Arbeiten wie Videoschnitt, Audioproduktion oder beim Hantieren mit riesigen Tabellen kann es hilfreich sein zu verstehen, warum die Hardware an ihre Grenzen gelangt. In diesem Artikel richten wir auf dem Linux-Desktop ein solches Game-Overlay mit MangoHud ein und zeigen, was es kann und wie Sie es konfigurieren.

Auf Ihrem lokalen Linux-System müssen Sie das Tool selbst installieren und einrichten. Im Folgenden zeigen wir zwei Konfigurationswege: traditionell per gut dokumentierter Konfigurationsdatei oder mithilfe des grafischen Tools GOverlay.

MangoHud installieren

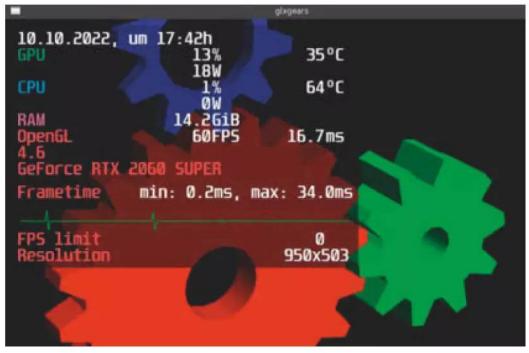
Die meisten Linux-Distributionen bieten das Tool in ihren Paketquellen an, sodass Sie das Paket „mangohud“ wie gewohnt mit der Software-Verwaltung installieren können. Unter Arch Linux installieren Sie die Software mit dem Kommando

```
sudo pacman -S mangohud
```

Fehlt MangoHud in den Repositories Ihrer Linux-Distribution, können Sie auf ein distributionsunabhängiges Flatpak zurückgreifen, die Installation beschreibt die Github-Seite des Projekts (siehe ct.de/wmkn).

Overlay anschalten

Frisch installiert bringt MangoHud eine Grundkonfiguration mit, die zum Ausprobieren allemal reicht. Bevor Sie sich in Details stürzen, sollten Sie sicherstellen, dass es funktioniert. Besonders einfach geht das mit den Testprogrammen Glxgears (für OpenGL) und Vkcube (für Vulkan), die bei vielen Distributionen meist schon an Bord sind. Fehlen sie, rüsten Sie die gleichnamigen Pakete aus den Paketquellen der Distribution nach.



Ein Testlauf mit Tools wie Glxgears zeigt, ob MangoHud funktioniert und dient als Vorschau bei der Konfiguration.

Um eine Software mit dem MangoHud-Overlay zu starten, stellen Sie dem Startbefehl in der Kommandozeile einfach den Aufruf `mangohud` voran. Also beispielsweise

```
mangohud glxgears
mangohud vkcube
```

Starten Glxgears oder Vkcube mit einem Overlay, hat alles geklappt und Sie können sich an die weitere Konfiguration machen.

Um das MangoHud-Overlay in einem Steam-Spiel zu nutzen, reicht ein ergänzender Startparameter. Klicken Sie dazu in der Steam-Bibliothek mit der rechten Maustaste auf das gewünschte Spiel, öffnen Sie die Eigenschaften und tragen Sie im Allgemein-Reiter ganz unten bei Startoption den Befehl `mangohud %command%` ein. Beim nächsten Spielstart erscheint das Overlay über dem Spielbild. Probieren Sie es ruhig erst mal aus.

Alternativ öffnen Sie Steam über die Kommandozeile und geben ihm dabei MangoHud mit auf den Weg (`mangohud steam`), dann ist das Overlay in allen Spielen automatisch an. Wie Sie ein Tastenkürzel definieren, um das Overlay jederzeit ein- oder ausschalten zu können, ohne Steam neu zu starten, erklären wir gleich.

MangoHud funktioniert auch mit Spielen, die Sie über das Gaming-Tool Lutris öffnen. Das Open-Source-Tool startet native Linux-Games ebenso wie solche, die mit Wine oder in Emulatoren laufen. Per Rechtsklick auf den Spieleeintrag und „Konfigurieren“ öffnen Sie die jeweiligen Einstellungen. Im Tab „Systemeinstellungen“ schieben Sie den Regler bei „FPS-Statusleiste (MangoHud)“ nach rechts und bestätigen mit „Speichern“. Beim nächsten Spielstart wird das Overlay angezeigt.

Infos nach Wunsch

Nach dem ersten Start zeigt MangoHud nur eine Handvoll Daten. In der Grundkonfiguration präsentiert das Tool Werte, die vor allem Gamer interessieren: die Auslastung von GPU und CPU in Prozent, die Anzahl der FPS (Frames per second) sowie die Frametime und ob OpenGL oder Vulkan (DXVK) zum Einsatz kommt. Um Einfluss auf die Anzeige zu nehmen, können Sie die gewünschten Parameter beim Programmstart mitgeben. Der folgende Befehl star-

tet beispielsweise Glxgears mit einem Overlay, das keine Werte für die Grafikkarte ausgibt und die Schriftgröße festlegt:

```
MANGOHUD_CONFIG="gpu_stats=0,\
font_size=12" mangohud glxgears
```

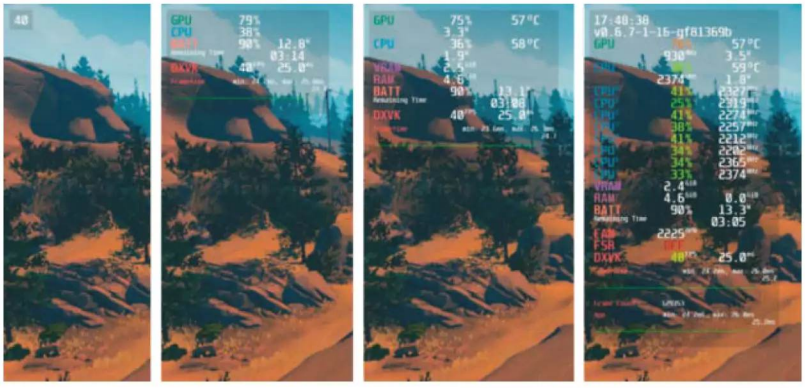
Um nur mal einen Parameter auszuprobieren, ist dieser Weg in Ordnung, auf Dauer aber zu umständlich. Hinterlegen Sie die Einstellungen besser in einer Konfigurationsdatei. Dort können Sie allgemeingültige Vorgaben für alle Programme machen, aber auch zusätzliche Konfigurationsdateien für einzelne Anwendungen definieren.

MangoHud durchsucht beim Start verschiedene Ordner nach einer passenden Konfiguration – zunächst /usr/bin, dann den Konfigurationsordner der Anwendung. Letzterer liegt in der Regel im versteckten Ordner .config im Home-Verzeichnis. Der Pfad zur globalen Konfigurationsdatei lautet dann ~/.config/MangoHud/MangoHud.conf. Möchten Sie für bestimmte Anwendungen eigene Konfigurationen anlegen, müssen diese den Namen des Programms und die Endung .conf tragen, für Glxgears also glxgears.conf.

Ein guter Startpunkt ist die mitgelieferte Beispielkonfiguration, die Sie nach der Installation im System unter /usr/share/doc/mangohud/MangoHud.conf oder auf der Github-Seite des Projekts finden (siehe ct.de/wmkn). Kopieren Sie die Datei ins Home-Verzeichnis nach ~/.config/MangoHud/. Unter Umständen müssen Sie das Verzeichnis MangoHud erst noch anlegen. Dann lauten die beiden Befehle beispielsweise wie folgt:

```
mkdir -p ~/.config/MangoHud
cp /usr/share/doc/mangohud/MangoHud
  .conf.example ~/.config/MangoHud/
  MangoHud.conf
```

In der Konfigurationsdatei steht jede Option in einer eigenen Zeile. Die Beispielkonfiguration enthält bereits viele Einstellungen, die Sie nur noch an- oder abschalten müssen. Die meisten Zeilen sind mit einem Doppelkreuz # am Anfang der Zeile bereits auskommentiert und damit inaktiv. Für einen Test entfernen Sie einfach probeweise vor einer Zeile das Kommentarzeichen, speichern die Datei und starten `mangohud glxgears`, um das Ergebnis im Overlay zu sehen. Nun können Sie die Konfigurationsdatei nach Herzenslust anpassen und experimentieren.



Das Steam Deck bringt ein Overlay mit, dessen Stufen unterschiedlich viele Infos zeigen. Mit MangoHud können Sie das meiste davon auf dem PC nachbauen.

Wie auf dem Steam Deck

Was Valve auf dem Steam Deck ab Werk bietet, können Sie mit wenigen Handgriffen weitgehend nachbauen (siehe Screenshot oben). Einen Schieberegler zum Umschalten zwischen den Konfigurationen gibt es am Desktop allerdings nicht.

Die einfachste Variante des Steam-Deck-Overlays zeigt lediglich die FPS ohne Beschriftung. Eine analoge Option fehlt in der Beispielkonfiguration von MangoHud. Kommentieren Sie daher alles aus (bis auf Tastenkürzel, die Sie nutzen wollen) und tippen Sie an beliebiger Stelle folgende Zeile ein:

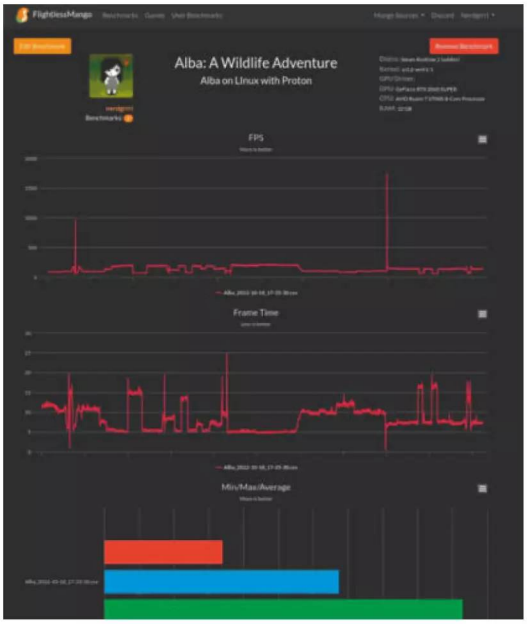
```
fps_only
```

Wenn Sie die Datei gespeichert und MangoHud erneut aufgerufen haben, ziert eine schlichte FPS-Zahl das Overlay.

Position Zwei des Steam-Deck-Schiebereglers ähnelte in früheren Versionen der ursprünglichen Beispielkonfiguration, wie sie oben im Screenshot zu sehen ist. Folgende Zeilen müssen Sie dafür noch ergänzen:

```
gpu_stats
cpu_stats
battery
fps
frame_timing
```

Der Parameter `battery` behält auf Notebooks den Akkustand im Blick. Seit einem SteamOS-Update liegen die Performance-Werte auf dem Steam Deck in Stufe 2 in einer Leiste am oberen Displayrand. Das erreichen Sie mit dem zusätzlichen Parameter `horizontal`. Mit `table_columns=30` können Sie dann die



Kurve statt Tabelle: Lädt man die Logdatei von MangoHud auf die Website des Entwicklers hoch, veranschaulicht diese das Ergebnis in Kurven und Balkendiagrammen.

Breite der Spalten beeinflussen. Für die Steam-Deck-Ansicht Numero 3 fügen Sie unterhalb von `cpu_stats` noch die Zeilen `vram` und `ram` hinzu.

Nur die vierte Variante des Steam-Deck-Overlays lässt sich nicht ganz nachbauen, da MangoHud beispielsweise keine Lüfterdrehzahlen auslesen kann. Eine ähnlich ausführliche Ausgabe liefert die Zeile `full`. Dann zeigt MangoHud zusätzlich die Uhrzeit (Parameter `time`), die MangoHud-Version (`version`), Temperaturen (`gpu_temp` und `cpu_temp`) sowie einiges mehr an. Möchten Sie Daten aller Prozessorkerne sehen und diese je nach Last von Grün über Gelb nach Rot einfärben, fügen Sie beispielsweise folgende Zeilen hinzu:

```
core_load
core_load_change
cpu_load_value=60,90
cpu_load_color=39F900,FDFD09,B22222
```

Darüber hinaus listet die Github-Seite von MangoHud weitere praktische Optionen auf. Sie können

etwa die verwendeten Farben anpassen, beispielsweise zeigt `gpu_color=666666` die Bezeichnung „GPU“ in Dunkelgrau an. Auch die Beispielkonfiguration zeigt einige Möglichkeiten auf. Experimentieren Sie ruhig, MangoHud ignoriert fehlerhafte Optionen.

Anders als auf dem Steam Deck fehlt ein Schalter für MangoHud, um es nur bei Bedarf anzuschalten. Definieren Sie dafür am besten ein Tastenkürzel:

```
toggle_hud=Shift_R+F12
```

Fortan knipsen Sie das Overlay mit der rechten Umschalttaste+F12 an oder aus.

Mitschreiben

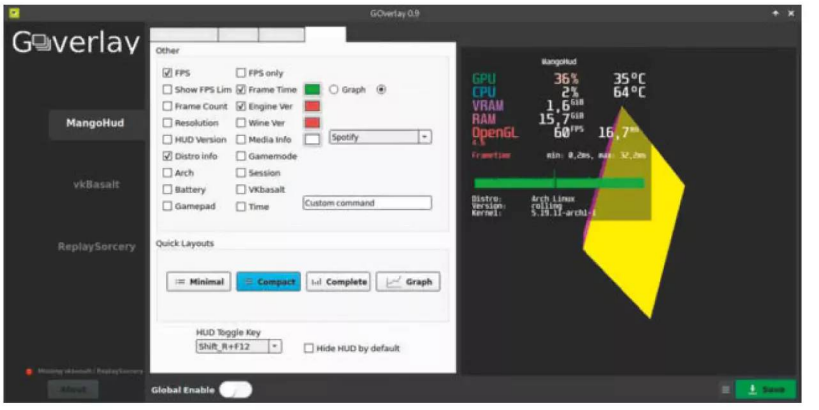
Falls gewünscht, schreibt MangoHud die erfassten Werte in eine CSV-Tabelle, die Sie später auswerten, für Vergleiche heranziehen oder als Datenbasis für Diagramme nutzen können. Damit das funktioniert, müssen Sie mit `output_folder=` zunächst ein Ausgabeverzeichnis für die Logdateien festlegen. Sie können MangoHud anweisen, das Mitschreiben nach einer Weile an- und wieder abzuschalten oder dafür eine Taste drücken (beispielsweise mit `toggle_logging=Shift_L+F2`).

Wollen Sie die Daten nicht selbst grafisch aufbereiten, laden Sie sie auf flightlessmango.com hoch. Im Nu erstellt die Website daraus Kurven und Balkendiagramme. Voraussetzung ist die Zeile `permit_upload=1`. Drückt man, während MangoHud läuft, die (etwa mit `upload_log=F5` definierte) Taste zum Upload, muss man dafür keinen Account anlegen. Die Seite mit den Grafiken öffnet sich danach automatisch im Browser.

Alternativ loggen Sie sich mit einem Discord-Account auf flightlessmango.com ein, suchen unter „User Benchmarks“ nach dem gewünschten Spiel und fügen mit „New Benchmark“ eigene Logdateien samt Kommentar hinzu. Der Vorteil: Sie können aus mehreren Logdateien gemeinsame Kurven erzeugen und später weitere hinzufügen. Das kann den Unterschied zwischen unterschiedlichen Messungen, Spieleinstellungen oder Hardware grafisch veranschaulichen.

Grafische Oberfläche GOverlay

Mit dem grafischen Frontend GOverlay ändern Sie die Einstellungen für MangoHud per Mausklick. In der Programmoberfläche sind zwar nicht alle, aber doch ziemlich viele Optionen verfügbar. Auch dieses Tool können Sie als Paket „goverlay“ über den Paketmanager Ihrer Linux-Distribution nachinstallieren. Unter Arch Linux und Manjaro installieren Sie es am einfachsten aus dem AUR mit dem Befehl `yay -S goverlay-bin`.



Grafische Oberfläche für MangoHud: In GOverlay klicken Sie das gewünschte Overlay schnell zusammen.

Anleitungen für Distributionen, in deren Paketquellen das Tool fehlt, gibt es auf der Github-Seite (siehe ct.de/wmkn). Sie starten es über das Anwendungsmenü oder mit dem Befehl `goverlay &`. In vier Tabs haken Sie nun einfach an, was Sie im Overlay sehen wollen und klicken rechts unten auf „Save“. Speichern Sie ruhig zwischendurch, GOverlay aktualisiert dann die Vorschau rechts. Im letzten Tab legen Sie eine Tastenkombination fest, mit der Sie das MangoHud-Overlay schnell ein- und wieder ausschalten. Standardmäßig ist dafür die linke Umschalttaste+F12 vorgesehen.

Außerdem sind hier bereits vier Layouts vorkonfiguriert: Minimal, Compact, Complete und Graph. Während sich Minimal auf die Frames konzentriert, präsentiert Compact Messdaten zu CPU, GPU, RAM, VRAM und FPS. Complete listet nicht nur sämtliche Prozessorkerne einzeln auf, sondern zeigt viele weitere Details. Spartanische Graphen zeigt die Konfiguration Graph.

Praktischer Helfer

Bringt die neue Grafikkarte wirklich so viel mehr? Ist doch noch ein neuer Prozessor fällig? MangoHud kann dazu beitragen, Antworten auf diese Fragen zu finden. Das Open-Source-Tool ist leicht einzurichten und an die eigenen Bedürfnisse anzupassen. Ein großer Vorteil sind die Benchmark-Ergebnisse auf der Projekt-Website, die auch dabei helfen können, die besten Grafikeinstellungen für ein Spiel zu ermitteln. (lmd) c't

Literatur

[1] Liane M. Dubowy, Taschenspielerei, Mobile Steam-Bibliothek: Spielkonsole Valve Steam Deck im Test, c't 9/2022, S. 112

Tools & Benchmarks

ct.de/wmkn

Jetzt gibt's eine aufs Dach!

Heft + PDF mit 26 % Rabatt

In diesem c't-Sonderheft fassen wir für Sie zusammen, was Sie für den Einstieg und die Planung von kleinen Photovoltaik-Anlagen wissen müssen. Es zeigt vor allem wie einfach es ist, beispielsweise ein 600 Watt Balkonkraftwerk in Betrieb zu nehmen. Darauf können Sie sich freuen:

- ► So kann jeder Stromkosten senken
- ► Das eigene Balkonkraftwerk
- ► Ertrag und Verbrauch im Blick
- ► Photovoltaik für alle
- ► Mikrowechselrichter kaufen und einsetzen
- ► Auch als Angebots-Paket Heft + PDF + Buch "Photovoltaik - Grundlagen, Planung, Betrieb" erhältlich!

Heft für 19,90 € • PDF für 16,90 € • Bundle Heft + PDF 26,90 €

shop.heise.de/ct-solarstromguide23

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 € (innerhalb Deutschlands). Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

heise Shop

Audioströme bequem umleiten mit PipeWire

Mit PipeWire wandeln Sie Ihren Linux-Computer im Handumdrehen zum heimischen Tonstudio um. Statt sich mit dem Soundserver JACK rumzuplagen, können Sie sich direkt in die erste Aufnahme-Session stürzen. Wir zeigen, wie Sie das neue Multimedia-Framework PipeWire installieren und ein Skype-Interview in getrennten Tonspuren mitschneiden.

Von **Alexander von Westernhagen**

Bild: Albert Hulm

Sowohl die finanzielle als auch die technische Hemmschwelle wird für angehende Musikproduzenten im Zeitalter erschwinglicher USB-Audio-Interfaces immer niedriger. Auch Linux-Anwender können professionelle Mehrspuraufnahmen produzieren – und das auch ausschließlich mit Open-Source-Tools. Um die Audiosignale auseinanderzudröseln und mit niedrigen Latenzen zu arbeiten, verlangen bessere Recording-Programme unter Linux meist die Schnittstellen des Soundservers JACK. Doch den zur Mitarbeit zu bewegen, hat selbst manchen gestandenen Linux-Anwender in die Verzweiflung getrieben oder erwies sich im Alltag einfach als unhandlich.

Glücklicherweise gehört die teils mühselige Konfiguration des Audiosystems an die speziellen Bedürfnisse des Recordings nun der Vergangenheit an. Denn das Multimedia-Framework PipeWire ersetzt bisher konkurrierende Audiosysteme und bringt eine eigene JACK-Implementierung mit. Und wo man früher für aufwendige Audioproduktionen noch einen Echtzeit-Kernel bemühen musste, reicht heutzutage der Standard-Kernel einer gängigen Distribution wie Ubuntu, da dieser schnell genug reagiert. Zudem sind viele USB-Geräte mit Linux kompatibel. Mit einem entsprechenden USB-Audio-Interface sind Sie bereits innerhalb weniger Minuten startklar für eine Mehrspuraufnahme.

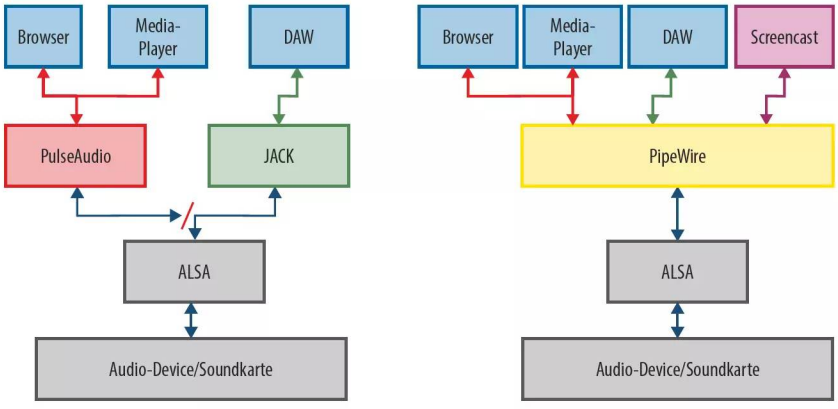
Wir erklären in diesem Artikel, was PipeWire ist und wie Sie es einrichten. Außerdem zeigen wir Ihnen, wie Sie die Tonausgabe einer beliebigen Anwendung als Audioquelle in die Aufnahmesoftware leiten. Für Übersicht bei den Begriffen sorgt das „Glossar: Linux-Audio“ auf Seite 58.

Das Linux-Audio-Ökosystem

Die Audiosignal-Verarbeitung unter Linux übernehmen verschiedene Komponenten, die teilweise aufeinander aufbauen, teilweise sich aber auch gegenseitig ausschließen oder blockieren. Dabei bildet ALSA die Treiberschicht im Kernel (siehe „Glossar: Linux-Audio“ auf Seite 58). Darauf bauen Soundserver wie PulseAudio oder JACK auf, die den Zugriff auf die Hardware abstrahieren und für Anwendungen einheitliche Schnittstellen bereitstellen. Während PulseAudio auf die Bedürfnisse von Desktop-Usern zugeschnitten ist, richtet sich JACK nach den Anforderungen professioneller Anwender.

PipeWire übernimmt

Bisher musste man sich entscheiden, ob JACK oder PulseAudio als Soundserver Zugriff auf das Audio-Device bekommt (links). Deren Rolle übernimmt nun das Multimedia-Framework PipeWire (rechts). Damit lassen sich PulseAudio- und JACK-Clients nicht nur gleichzeitig verwenden, sondern deren Audiosignale auch miteinander verbinden. PipeWire stellt Anwendungen die gewohnten Schnittstellen bereit, sodass die Programme sich ohne Anpassung weiter nutzen lassen.



Glossar: Linux-Audio

DAW steht für Digital Audio Workstation und bezeichnet meist eine Software, in der mehrspurige Audioaufnahmen erstellt und bearbeitet werden können. Viele DAWs nehmen auch MIDI-Spuren auf beziehungsweise erlauben deren Programmierung. Eine verbreitete DAW unter Linux ist Ardour.

Die **Advanced Linux Sound Architecture (ALSA)** ist Teil des Linux-Kernels und besteht aus einer Sammlung von Treibern. Die lädt der Kernel beim Booten oder zur Laufzeit, passend zur vorhandenen Soundkarte respektive zum verwendeten Audio-Interface. ALSA arbeitet mit den meisten USB-Audio-Interfaces zusammen, die komplexe Konfiguration schreckt Einsteiger jedoch ab. Außerdem kann nur ein Programm gleichzeitig auf die ALSA-Schnittstelle zugreifen, weshalb sich Soundserver wie PulseAudio oder JACK als Mittler etabliert haben.

Der Soundserver **PulseAudio** war bisher der Standard der meisten gängigen Linux-Distributionen. Diese Middleware kommuniziert zwischen den Audioanwendungen und den ALSA-Treibern und hat den Umgang mit Audiosoftware vereinfacht. PulseAudio erlaubt die parallele Nutzung desselben Audiogerätes durch mehrere Programme (Clients) ebenso wie die Aufteilung der Tonsignale auf verschiedene Ausgänge. Auch die meisten DAWs eignen sich als PulseAudio-Clients, doch die Kombination überfordert die CPU schnell, gerade wenn viele Echtzeiteffekte gleichzeitig genutzt werden.

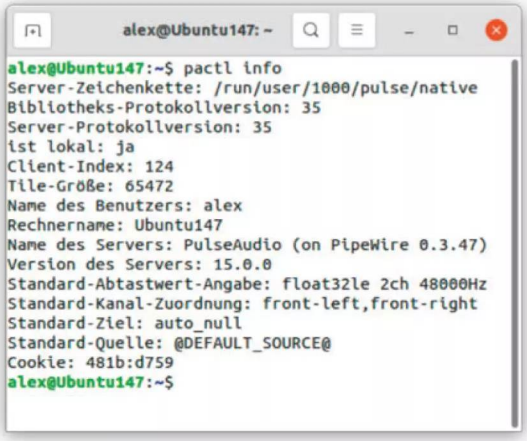
Das **Jack Audio Connection Kit (JACK)** wurde speziell für Audioproduktionen entwickelt. Audioanwendungen und DAWs arbeiten damit viel flüssiger und mit niedrigeren Latenzen. Die Anwendungen müssen dazu aber das JACK-Protokoll unterstützen, was auf viele Programme nicht zutrifft. Zusätzliche Anwendungen wie QjackCtl erlauben, alle Audio- und MIDI-Signale der mit JACK verbundenen Anwendungen zu verschalten und diese Konfigurationen als Presets zu speichern. JACK muss in der Regel manuell gestartet werden, ist nicht ganz leicht zu konfigurieren und blockiert auf von ihm genutzten Audio-Interfaces die Klangwiedergabe aller Anwendungen, die nicht mit ihm kommunizieren.

PipeWire ist ein relativ neues Multimedia-Framework, was ursprünglich nur für Videoströme gedacht war. Es erlaubt die gleichzeitige Nutzung von Programmen, die JACK-, PulseAudio- oder ALSA-Schnittstellen verwenden. Wo Programme es anfordern, verarbeitet PipeWire Audioströme mit niedrigen Latenzen. Selbst Anwendungen, die in einer Sandbox laufen, wie beispielsweise als Flatpak installierte Apps, sind hier ohne viel Konfigurationsaufwand gemeinsam nutzbar. Dazu können alle Signale frei miteinander verdrahtet werden, sodass man alle zur Verfügung stehenden Audioquellen wie Browser oder Videoplayer zur Aufnahme in eine DAW leiten kann. Die gängigen Distributionen wie Fedora oder Ubuntu nutzen mittlerweile PipeWire als Standard-Audioschnittstelle.

Einen Mittelweg geht das Multimedia-Framework PipeWire: Es verarbeitet wo nötig mit geringen Latenzen wie JACK, lässt sich aber einfacher konfigurieren. Praktischerweise stellt PipeWire die Schnittstellen von PulseAudio und JACK bereit, weshalb vorhandene Programme ohne Anpassung auch mit PipeWire zusammenspielen. Mehr noch: Anwendungen für die konkurrierenden Schnittstellen lassen sich sogar parallel nutzen und ihre Kanäle untereinander verbinden.

Installation

Aktuelle Versionen mancher Distributionen wie etwa Ubuntu 22.04 LTS haben PipeWire bereits an Bord, lassen es allerdings zugunsten von PulseAudio noch deaktiviert. Fedora hat hingegen PulseAudio mit Version 34 gegen PipeWire ausgetauscht. Ansonsten lässt sich PipeWire meist über das Paket „pipewire“ nachinstallieren. Damit auch alle anderen Audioanwendungen wie Musik- oder Video-Player rei-



Installation geglückt: PipeWire arbeitet als PulseAudio-Server und ist bereit, Audiosignale in alle Richtungen umzuleiten.

bungslos mit PipeWire laufen, sollten Sie in jedem Fall noch zusätzliche Bibliotheken für Bluetooth, GStreamer und JACK installieren. Gerade Letztere benötigen Sie, um Recording-Software (DAWs) mit JACK-Unterstützung sinnvoll zu nutzen. Unter Ubuntu geben Sie dazu den folgenden Befehl ein:

```
sudo apt install pipewire pipewire-pulse \
     pipewire-audio-client-libraries \
     gstreamer1.0-pipewire libspa-0.2-bluetooth
```

Es ist nicht nötig, zusätzlich JACK-Bibliotheken oder gar den JACK-Daemon zu installieren. Auch das manchmal empfohlene Paket „libspa-0.2-jack“ benötigen Sie nicht, da es dazu dient, PipeWire als JACK-Client mit einem anderen JACK-Server zu verbinden. Die serverseitige JACK-Implementierung von PipeWire kommt in Ubuntu mit dem Paket „pipewire-audio-client-libraries“. Unter Fedora machen Sie einen Bogen um „pipewire-plugin-jack“ und installieren stattdessen „pipewire-jack-audio-connection-kit“.

Starten Sie anschließend den Computer neu, damit PipeWire den PulseAudio-Server ersetzt. Prüfen Sie danach, ob die Installation erfolgreich war. Rufen Sie dazu in einem Terminal mit `pactl info` die PulseAudio-Informationen auf. In der Zeile „Name des Servers“ sollte „PulseAudio (on PipeWire 0.3...)“ stehen.

JACK-Clients mit PipeWire verbinden

PipeWire verfügt über eine eigene JACK-Implementierung und fungiert als Drop-In-Ersatz für JACK. In der Regel sollten JACK-Clients wie eine DAW ohne weiteres Zutun PipeWire als JACK-Server erkennen. Starten Sie ein Programm wie Ardour und wählen Sie als Audiosystem JACK aus. Erkennt Ardour in PipeWire eine JACK-Instanz, meldet es, der JACK-Server sei bereits gestartet. Stellen Sie die gewünschte Puffergröße ein und klicken Sie gegebenenfalls noch auf „verbinden“.

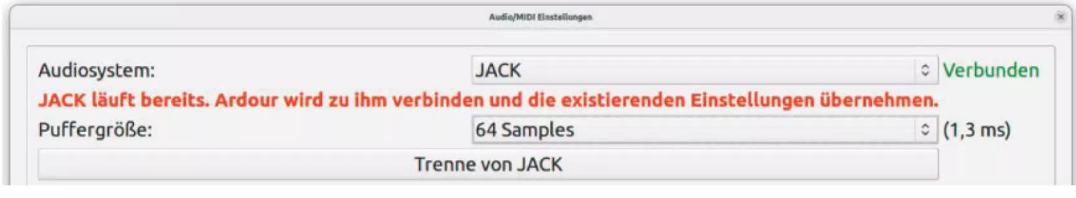
Sollte Ardour nicht an PipeWire als JACK-Instanz ankoppeln, versuchen Sie nicht, den JACK-Server über den Ardour-Dialog zu starten. Forcieren Sie stattdessen die Verbindung mit einem Trick: Öffnen Sie ein Terminal und starten Sie Ardour mit dem Befehl `pw-jack ardour` explizit als JACK-Client unter PipeWire. Das Skript `pw-jack` modifiziert temporär eine Umgebungsvariable und stößt Anwendungen so auf die PipeWire-Bibliotheken.

Schaltzentrale

Um mehr Kontrollmöglichkeiten über alle Audio- und MIDI-Ströme zu gewinnen, installieren Sie das Programm qpwgraph. Der sperrige Name steht für „Qt PipeWire Graph“ (Q-PW-Graph). Es ist eine virtuelle Schaltzentrale für PipeWire und gleicht dem Graph-Tool von QjackCtl für JACK. Am einfachsten lässt sich qpwgraph über Flatpak installieren. Dieses Paketverwaltungs-Tool müssen Sie vorher in Ubuntu installieren, falls nicht bereits geschehen:

```
sudo apt install flatpak
```

Richten Sie anschließend in Flatpak die Paketquelle Flathub ein und installieren aus dieser dann qpwgraph:



Die Recording-Software Ardour hat eine JACK-Instanz erkannt, ohne zu wissen, dass die zu PipeWire gehört.

```
flatpak remote-add --if-not-exists flathub \
      https://flathub.org/repo/flathub.flatpakrepo
flatpak install org.rncbc.qpwgraph
```

Wenn Sie qpwgraph starten, sehen Sie die Ein- und Ausgänge (Streams) aller Programme und Geräte, die mit PipeWire verbunden sind. In qpwgraph sind alle Audio- und MIDI-Streams visuell dargestellt. Falls Sie nur ein Kuddelmuddel sehen, schieben Sie die einzelnen Objekte etwas auseinander. Die Ein- und Ausgänge können Sie nach Belieben per Drag & Drop verschalten. Sogar Signale von verschiedenen Interfaces können Sie nun zu einer Anwendung routen. Die Schalt-Patches können Sie abspeichern und später wieder laden. In qpwgraph erkennen Sie am kleinen PW-Logo, dass die Instanz von Ardour über PipeWire läuft. Es ist also alles startklar für das erste Audioprojekt.

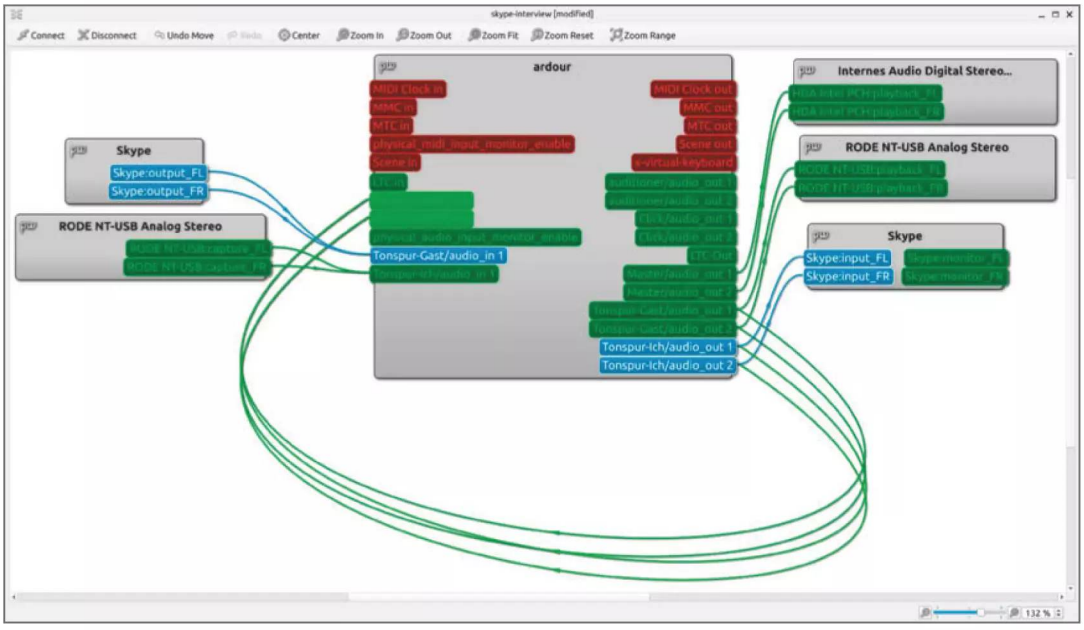
Falls Ihnen qpwgraph zu unübersichtlich ist, probieren Sie Helvum aus, das ähnlich funktioniert. Auch Helvum finden Sie im Flathub-Repository.

Die erste Aufnahme

Mit Hilfe von qpwgraph (oder Helvum) können Sie den Ton eines im Browser laufenden Videos direkt in der DAW aufnehmen, um es beispielsweise als Sample zu verwenden. Zwar bieten professionelle Programme wie Ardour selbst Werkzeuge an, mit denen Sie Audiosignale in die gewünschte Tonspur umleiten können. Aber die Visualisierung von qpwgraph veranschaulicht die Arbeitsweise von PipeWire greifbarer.

In qpwgraph sehen Sie alle verfügbaren Audiosignale als grüne Kästchen, links die Eingänge, rechts die Ausgänge. Die Eingänge der Audiogeräte (Mikrofon, Input, ...) sind normalerweise automatisch mit dem Eingang des Aufnahmeprogramms Ardour verdrahtet. Legen Sie in Ardour nun eine neue Stereo-Audiospur an und nennen diese zum Beispiel „Tonspur“ (siehe Artikel „Einstieg in die freie DAW Ardour“ auf S. 62). Starten Sie dann im Browser das Video, worauf in qpwgraph für den Browser ein neues Element erscheint. Verbinden Sie nun in qpwgraph per Drag & Drop den Browser-Ausgang („Firefox:output FL“) mit der Ardour-Spur („Tonspur/audio_in 1“). Wiederholen Sie das auch für die rechte Spur („Firefox:output FR“ mit „Tonspur/audio_in 2“). Wenn Sie jetzt die Aufnahme in Ardour starten, landet das Audiosignal des Browservideos direkt in der gewünschten Audiospur.

Nach dem gleichen Prinzip können Sie auch eine Skype-, Teams- oder Zoom-Unterhaltung in einer hohen Qualität mitschneiden, etwa als Interview für



Mit qpwgraph verdrahten Sie in PipeWire die Audiosignale und -kanäle beliebiger Anwendungen bequem per Drag & Drop.

Konfiguration: JACK verdrahtet

Damit Sie nicht bei jedem Start von Ardour die JACK-Einstellungen anpassen müssen, können Sie diese in einer Konfigurationsdatei vorab festlegen. Es ist aber empfehlenswert, zuerst in Ardour mit den Werten zu experimentieren (siehe Artikel „Einstieg in die freie DAW Ardour“ auf S. 62). Haben Sie die passenden Werte ermittelt, tragen Sie diese in der Konfigurationsdatei ein. Eine Vorlage finden Sie unter „/usr/share/pipewire/jack.conf“. Kopieren Sie die Datei in Ihr Home-Verzeichnis, wobei Sie den dafür vorgesehenen Unterordner („.config/pipewire“) vermutlich erst erstellen müssen. Im Terminal nutzen Sie dafür folgende Befehle:

```
mkdir -p ~/.config/pipewire
cp -i /usr/share/pipewire/jack.conf \
      ~/.config/pipewire/
```

Öffnen Sie anschließend die Datei mit Ihrem bevorzugten Texteditor. In dieser Konfigurationsdatei können Sie sämtliche Standardeinstellungen für JACK-Anwendungen verwalten. Interessant für den Recording-Bereich sind insbesondere die Einstellung der Puffergröße und der Samplerate des Audiosignals. Springen Sie in der Datei direkt zum Bereich „global properties for all jack clients“. In der Zeile `node.latency` legen Sie die gewünschte Puffergröße fest, mit `node.rate` die Samplerate. Durch das Entfernen der Raute (#) aktivieren Sie die auskommentierte Zeile. Tragen Sie hier die gewünschten Werte ein:

```
node.latency = 128/48000
node.rate    =   1/48000
```

Speichern Sie die Datei ab. Bei der nächsten Verbindung mit PipeWires JACK-Instanz hat Ardour den definierten Wert voreingestellt. Möchten Sie die Konfiguration systemweit für alle Benutzer festlegen, kopieren Sie die Konfigurationsdatei nach „/etc/pipewire/jack.conf“, wofür Sie Root-Rechte benötigen.

einen Podcast. Das Vorgehen ist ähnlich, jedoch können Sie für sich und Ihren Gesprächspartner den Ton in separaten Audiospuren aufnehmen. Das erlaubt Ihnen, später Ihre Stimme und die Ihres Gesprächspartners getrennt voneinander zu bearbeiten. Lautstärke-, Dynamik- und Equalizer-Unterschiede gleichen Sie so bequem nachträglich an und Ihr Podcast-Mix klingt am Ende viel professioneller.

Legen Sie dazu in Ardour zwei Mono-Audiospuren an und benennen Sie diese Tonspuren eindeutig. Starten Sie in Skype das Gespräch oder einen Testanruf. Ihr Mikrofon, welches Sie zur Skype-Unterhaltung benutzen, leiten Sie zusätzlich auf die erste Mono-Spur. Das Signal der Skype-Audioausgabe legen Sie als Quelle für Ihre zweite Spur fest. Hierbei gibt es eine Besonderheit zu beachten: Anwendungen, die auf Chromium-Basis laufen – wie in diesem Beispiel Skype für Linux – tauchen auch in der Signalverwaltung unter dessen Namen auf. Aber Skype spielt über den Chromium-Kanal nur Benachrichtigungsklänge ab, nicht den Anruf selbst. Definieren Sie „Skype:output“ als Audioquelle der zweiten Spur. Kappen Sie in qpwgraph gegebenenfalls auch direkte Verbindungen von Skype und Ihrem Mikro zu Lautsprechern, um Rückkopplungen vorzubeugen. Nun kann die Aufnahme in getrennten Spuren starten.

Kinderleichtes Routing

Mit PipeWire können Sie den Ton von Streams und Videocalls auch zu beliebigen anderen Anwendungen weiterleiten, solange die über Ein- und/oder Ausgangskanäle verfügen. Statt Ardour könnten Sie für die Aufnahme den simplen „Tonaufzeichner“ von Gnome nehmen, obwohl man dort die Audioquelle nicht auswählen kann. Oder Sie leiten aus VLC den Ton eines Videoclips um zu Skype, um das Audiosignal für Ihren Gesprächspartner einzuspielen. Selbst manch ein Mac-verwöhnter Studio-Nerd dürfte angesichts PipeWires kinderleichtem Signal-Routing begeistert sein.

Einen Einstieg in die vielseitige Recording-Anwendung Ardour bietet der nächste Artikel. Darin zeigen wir Ihnen, wie Sie mit Ardour einen eigenen Song aufnehmen und abmischen. (ktn) c't

Pipewire-Dokumentation
ct.de/we4g

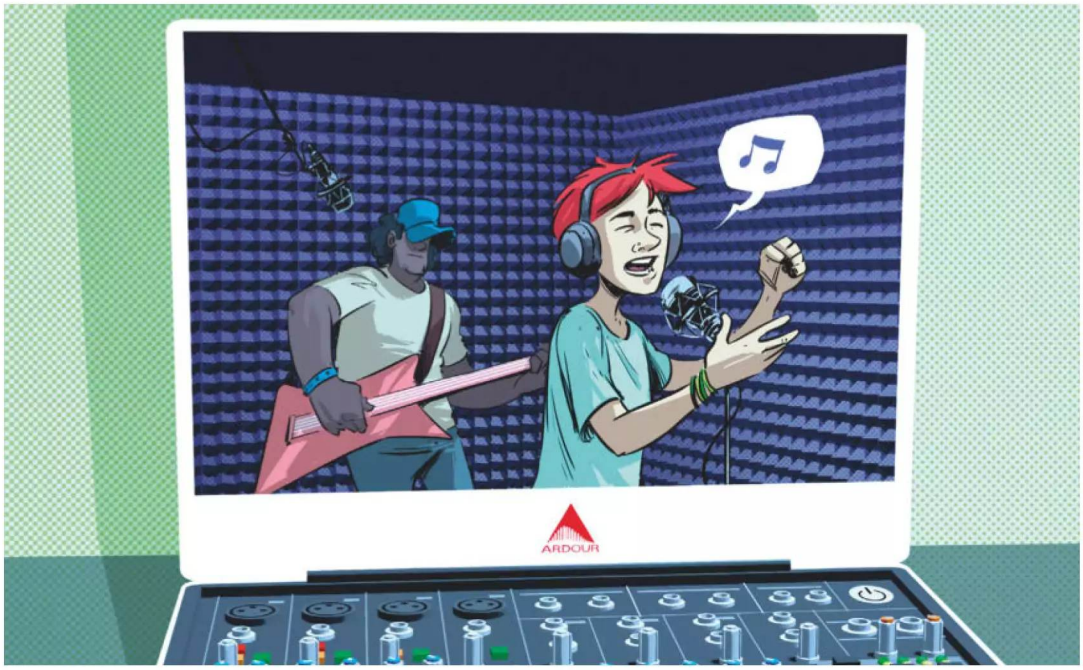


Bild: Albert Hulm

Einstieg in die freie DAW Ardour

Die Linux-Community liebt Ardour als Anwendung für Audioaufnahmen und Musikkomposition. Die Open-Source-Software stellt mit ihrem Funktionsumfang auch anspruchsvolle Produzenten zufrieden. Wir zeigen Ihnen, wie Sie mit Ardour aufnehmen, einen Beat programmieren und Ihr erstes Musikstück exportieren.

Von **Alexander von Westernhagen**

Für Audioproduktionen hat sich die freie Recording-Software Ardour einen Namen gemacht. Für kleines Geld, teils auch kostenlos, bietet sie einen erstaunlichen Funktionsumfang. Doch für Einsteiger kann Ardour, wie fast jede Digital Audio Workstation (DAW), verwirrend sein. Daher erklären wir Ihnen in diesem Artikel die wichtigsten Tools und Einstellungen und zeigen Schritt für Schritt, wie Sie Ihren ersten Beat programmieren, Aufnahmen einspielen, abmischen und schlussendlich Ihr erstes Musikstück exportieren. Loslegen können Sie bereits mit dem integrierten Sound-Interface („Soundkarte“) Ihres Computers. Ein USB-Audio-Interface benötigen Sie erst, wenn Sie physische Instrumente einspielen oder in ein Mikrofon singen wollen. Zum Abhören genügt zunächst ein möglichst neutral klingender Kopfhörer.

Installation

Ardour ist Open Source; auf der Projektwebseite kostenlos zum Download gibt es aber nur den Quelltext. Für fertig ausführbare Programme und Setup-Dateien für Windows, macOS und Linux verlangt das Projekt eine Einmalzahlung oder ein Abonnement, deren Höhe man jeweils ab einem US-Dollar aufwärts selbst festlegen darf.

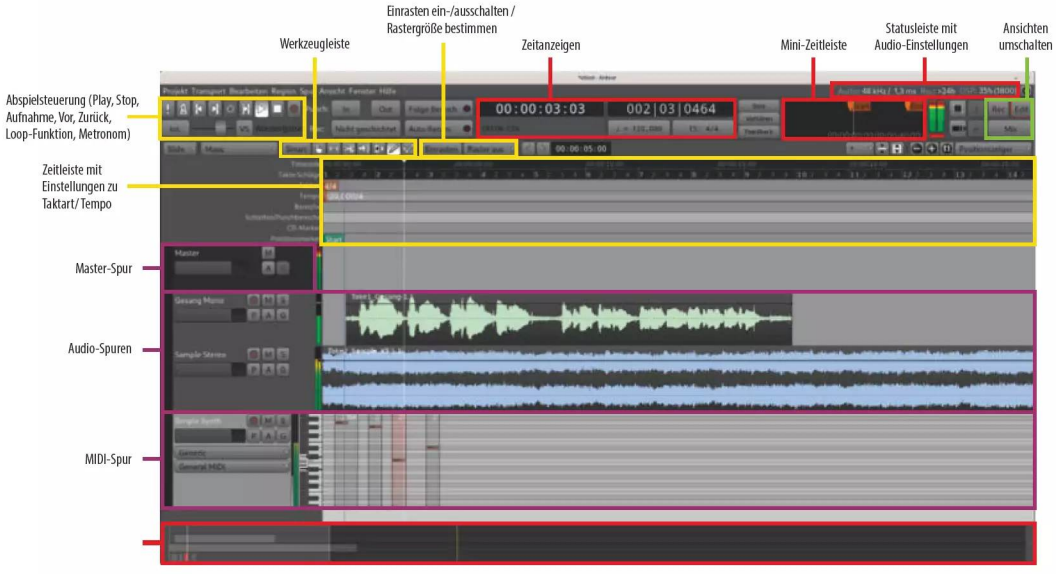
Alle gängigen Linux-Distributionen haben eine mehr oder weniger aktuelle Version von Ardour in ihren Paketquellen (zurzeit Version 7.5), die Sie über den Paketmanager kostenlos installieren können. Alternativ beziehen Sie die Linux-Version von Ardour als Flatpak über Flathub.org – ebenfalls kostenlos. Die Installation via Flatpak hat aber einen Nachteil: Da Ardour in diesem Fall in einer Sandbox läuft, werden außerhalb von Flatpak installierte Plug-ins nicht erkannt. Etliche Plug-ins sind aber auch im Flathub-Repository vorhanden. Welche das sind, zeigt im Terminal der Befehl `flatpak search LinuxAudio.Plugins`. Wie Sie Flathub einrichten, steht im Artikel „Audioströme bequem umleiten mit PipeWire“ auf Seite 56.

Apropos Plug-ins: Die Grundausstattung von Ardour mag jemandem, der nur leicht Lautstärke und Dynamik anpassen will, durchaus reichen. Möchte man jedoch etwas aufwendigere Musikproduktionen auf die Beine stellen, kommt man um zusätzliche Plug-ins nicht herum. Welche Formate Ardour unterstützt und wie diese sich unterscheiden, lesen Sie im Kasten „Plug-ins für Ardour“ auf Seite 65.

Für dieses Projekt benötigen Sie neben Ardour noch zwei Zusatz-Tools: Die „Calf Plugin Suite“ und den Sampler „samplv1“. Mit stattlichen 47 Plug-ins ist die Calf Suite wohl die umfangreichste Sammlung von Effekten und Instrumenten für Linux. Das Plug-in samplv1 benötigen Sie, um Samples zu laden, zu bearbeiten und abzuspielen. Statt Samples in Form von Audiodateien umständlich auf der Spur zu arrangieren, wird der Sampler wie ein Synthesizer via MIDI-Noteneingabe angesteuert. Das hat den Vorteil, dass man das Sample jederzeit gegen ein anderes ersetzen kann, ohne das Arrangement verändern zu müssen. MIDI-Arrangements können zudem einfach kopiert und verschoben werden, was die Bearbeitung und Wiederverwendung von Songteilen erleichtert.

Die Ardour-Bedienoberfläche

Ardour gliedert sich je nach Arbeitsschritt in unterschiedliche Ansichten wie Editor, Rekorder oder Mixer. Der hier dargestellte Editor eignet sich als zentraler Arbeitsbereich, um Lieder einzuspielen, zu arrangieren und zu bearbeiten, da man dort auch Aufnahmen steuern kann.



Um Ardour samt der genannten Plug-ins zu installieren, geben Sie unter Debian oder Ubuntu folgenden Befehl im Terminal ein:

```
sudo apt install ardour calf-plugins samplv1-lv2
```

Bei Fedora müssen Sie die Pakete `ardour6`, `lv2-calf-plugins` und `lv2-samplv1` installieren; bei Arch Linux heißen die Pakete `ardour7`, `calf` und `samplv1`. Alle Plug-ins befinden sich anschließend im Verzeichnis „/usr/lib/lv2“.

Einstellungssache

Öffnen Sie Ardour, fragt das Programm ab, ob Sie ein vorhandenes Projekt öffnen oder ein neues Projekt erzeugen möchten. Drücken Sie den Button „Neues Projekt“, woraufhin das nächste Fenster erscheint. Dort übernehmen Sie die „Leere Vorlage“, wählen den Speicherort aus und benennen das Projekt. Ardour speichert Projekte jeweils in einem eigenen Verzeichnis, wo alle Projektdateien wie Aufnahmen, Samples und Einstellungen gesammelt werden. Öffnen Sie das neue Projekt über die Schaltfläche „Open“.

Je nachdem, welches Audiosystem Sie nutzen, müssen Sie noch einige Einstellungen vornehmen. Unter Linux empfehlen wir die JACK-Implementierung von PipeWire, damit Sie mehrspurig und mit geringen Latenzen aufnehmen können. Wie Sie PipeWire als JACK-Ersatz einrichten, haben wir im Artikel „Audioströme bequem umleiten mit PipeWire“ auf Seite 56 beschrieben.

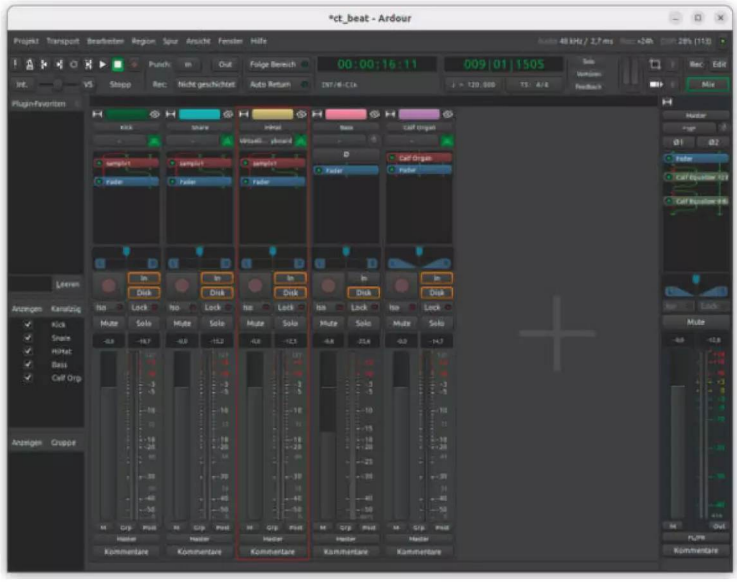
Standardmäßig startet Ardour eine Session mit der voreingestellten Samplerate des Audio-Interfaces und einer Puffergröße von 1024 Samples, was meist in einer Latenz (Signalverzögerung) im Bereich von 21 ms resultiert. Diese ressourcenschonende Voreinstellung mag für das spätere Mischen genügen. Möchten Sie hingegen mit einem MIDI-Keyboard zum laufenden Metronom Noten einspielen oder mit einem Mikrofon zum Playback eine Gesangsspur einsingen, ist diese Verzögerung viel zu hoch, da sie während der Aufnahme ein deutliches Echo erzeugt.

Generell gilt: Je kleiner die Puffergröße, desto geringer die Latenz. Die Puffergröße lässt sich in den JACK-Einstellungen bis auf 8 Samples herabsetzen, was auf unserem Testrechner und mit unserem Audio-Interface zu einer Latenz von nur 0,2 ms führte. Das Ganze bringt die CPU aber gehörig ins Schwitzen.

Wenn die CPU solche extremen Einstellungen nicht mitträgt, kommt es zu Knacksern und Aussetzern. Nähern Sie sich durch schrittweises Heraufsetzen der Puffergröße an einen optimalen Kompromiss zwischen Latenz und Last an. 64 bis 128 Samples sind ein guter Richtwert für störungsfreie Aufnahmen. Die mögliche Puffergröße variiert je nach verwendetem PC-Innenleben und Audio-Interface. Die Puffergröße können Sie jederzeit verändern, indem Sie in Ardour oben rechts in der Statusleiste auf die Audio-Informationen doppelklicken.

Tools und Ansichten

Bevor Sie loslegen, sollten Sie sich zunächst kurz mit den Tools von Ardour vertraut machen: Oben links befindet sich eine Leiste mit Transportwerkzeugen wie Play, Stop, Vor und Zurück. Dort schalten Sie auch das Metronom ein, das Sie als akustischer Taktgeber beim Einspielen und Einsingen von Spuren unterstützt. Dessen Taktvorgabe landet dabei nicht in der Aufnahme. Der Aufnahmeschalter versetzt das Playback in den Recording-Modus. Drücken Sie dann den Play-Button, nimmt Ardour aus den gewählten Quellen auf. Dazu müssen Sie vorher die jeweiligen Tonspuren mit deren Recording-Button scharf schalten.



In Ardours Mix-Ansicht weisen Sie den Spuren über Plug-ins Effekte und Instrumente zu und feilen wie im Tonstudio am richtigen Sound.

Direkt über der Zeitleiste gibt es eine Auswahl an Werkzeugen, die für die Bearbeitung von MIDI- und Audio-Objekten essenziell sind: Greifen, Auswählen, Schneiden, Vorhören, Strecken, Zeichnen und Automationen anlegen. Rechts davon ist die Funktion „Einrasten“, womit Sie MIDI-Noten exakt auf das Zeitraster setzen. Die Rastergröße gibt die Notenlängen vor, die Sie über das Drop-Down-Menü daneben festlegen. Unter der Taktanzeige stellen Sie die gewünschte BPM-Zahl und die Taktart ein. Diese Angaben können Sie auch in der Zeitleiste wählen. So ändern Sie Tempo und Takt auch mitten im Song.

Oben rechts wechseln Sie zwischen drei verschiedenen Ansichts-Modi von Ardour: Record, Edit und Mix. In der Rec-Ansicht treffen Sie alle für die Aufnahme relevanten Einstellungen. Die Edit-Ansicht ist fürs Arrangieren des Songs und die MIDI-Programmierung wichtig, eignet sich aber auch zur Steuerung von Aufnahmen. Die Mix-Ansicht zeigt in einer Übersicht alle Spuren und die darin verwendeten Plug-ins an.

Der erste Beat

Für einen einfachen Beat bestehend aus Kick, Snare und HiHat legen Sie zunächst drei MIDI-Spuren an. Eine neue Spur erzeugen Sie durch Rechtsklick in ein freies Feld unter der Master-Spur, woraufhin das Dialogfeld „Spur/Bus/VCA hinzufügen“ erscheint. In der Auswahl „Vorlage/Typ“ wählen Sie „Midispuren“ aus. Damit Sie die Spuren später gut zuordnen können, geben Sie diesen in den Kanaleinstellungen jeweils einen eindeutigen Namen wie „Kick“ oder „Snare“. Wählen Sie im Dropdown-Menü „Instrument“ den Sampler „samplv1“ aus, die restlichen Einstellungen belassen Sie wie von Ardour vorge-

Plug-ins für Ardour

Auch wenn der Plug-in-Markt für Linux viel kleiner ist als der für Windows oder macOS, sieht man sich zunächst mit einem Begriffswirrwarr rund um die Formate der Plug-ins konfrontiert. Immer wieder tauchen Begriffe wie VST, LADSPA und LV2 auf. Das sind die von Ardour unterstützten Formate.

VST (Virtual Studio Technology) ist ein proprietäres Plug-in-Format, das ursprünglich das Unternehmen Steinberg für das Sequenzer-Programm Cubase entwickelt hat. Durch die wachsende Popularität von Cubase etablierte sich das VST-Format als Quasi-Industriestandard. Plug-ins im VST-Format können sowohl Audio-Effekte als auch Software-Instrumente wie Synthesizer sein. Ardour unterstützt seit Version 6.5 auch VST3. Die meisten VST-Plug-ins sind allerdings nur für Windows und macOS verfügbar. Für Linux ist die Auswahl sehr viel kleiner. Notfalls kann man versuchen mit der Plug-in-Software Carla via Wine Windows-VSTs unter Linux zu laden.

Der etwas sperrige Begriff **LADSPA** steht für „Linux Audio Developer's Simple Plugin API“ und ist ein reines Linux-Format. Die bereits etwas in die Jahre gekommene Schnittstelle ermöglicht nur das Bearbeiten von Audiosignalen. Für MIDI-Verarbeitung beziehungsweise als Synthesizerformat fungierte DSSI (Disposable Soft Synth Interface) an der Seite von LADSPA. Beide Linux-Formate wurden mittlerweile weitestgehend vom Nachfolger **LV2** (LADSPA Version 2) abgelöst. Da es sowohl Audio als auch MIDI unterstützt und zudem individuelle Benutzeroberflächen erlaubt, ist LV2 eine ernstzunehmende Open-Source-Alternative zum proprietären VST.

Den neuen, offenen Plug-in-Standard **CLAP** (CLever Audio Plug-in) wird Ardour in absehbarer Zeit wohl nicht unterstützen, aber das Ardour-Team beteiligt sich beratend an der CLAP-Entwicklung.

Mit Open-Source-Plug-ins sind durchaus professionell klingende Mischungen möglich. Erst wenn man dort an klangliche Grenzen stößt, der Workflow einen zu sehr ausbremst oder man einen ganz bestimmten Synthesizer sucht, lohnt der Kauf kommerzieller Plug-ins.

geben. Das Ganze wiederholen Sie zwei weitere Male. Sollten Sie samplv1 nicht als Instrument finden, wählen Sie im Menü zunächst „-kein-“ aus.

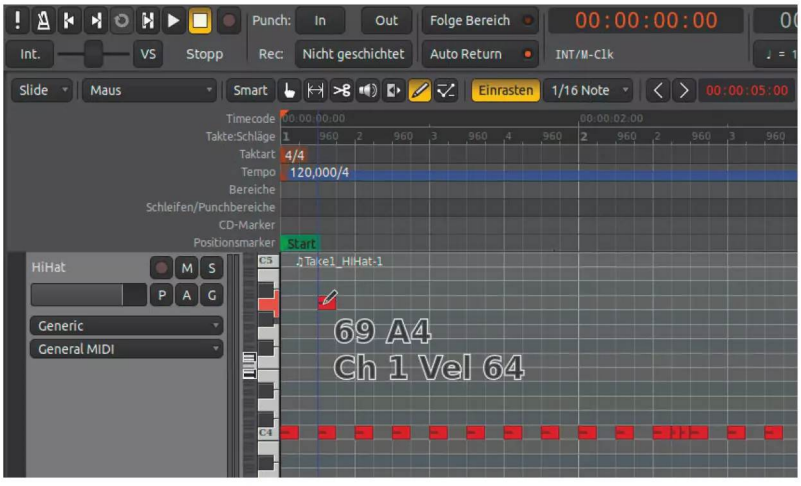
Wechseln Sie mit dem Ansicht-Umschalter in den Bereich „Mix“. Dort erscheint eine Übersicht der angelegten Kanäle samt der geladenen Plug-ins. Falls Ihnen samplv1 noch als Instrument fehlt, klicken Sie innerhalb der Spuren oberhalb des Blocks „Fader“ mit der rechten Maustaste und wählen aus dem Kontextmenü „Plugin einfügen/Nach Urheber/rncbc aka. Rui Nuno Capela/samplv1“ aus. Klicken Sie dann nochmal per Rechtsklick auf den samplv1-Block und öffnen Sie die Pin-Konfiguration. Dort aktivieren Sie die „Manuelle Konfiguration“ und fügen einen Audio-Ausgang über das Plus-Symbol hinzu. Nun sollte im Mix-Fenster ganz unten in der Spur als Ausgang „Master“ stehen.

Wenn samplv1 fertig konfiguriert ist, klicken Sie doppelt auf den samplv1-Block, um die Benutzeroberfläche des Samplers zu öffnen. Nun können Sie eine Audiodatei als Sample einbinden. Dazu ziehen Sie die Datei entweder per Drag & Drop auf den grauen Bereich „double-click or drop to load new sample“ oder öffnen dort per Doppelklick den Dateiauswahldialog. Alle weiteren Einstellungen des Samplers können Sie zunächst ignorieren.

Wir haben für das Beispielprojekt ein kostenloses Sample-Pack verwendet, das Sounds der legendären Drum-Machine Roland TR-808 enthält. Dieses Sample-Pack finden Sie auf der Webseite samplesfrommars.com als Download (siehe ct.de/wv5r). Es gibt unzählige weitere Webseiten und Foren, über die Sie kostenlose Drum-Samples erhalten. Oder Sie verwenden ein selbst aufgenommenes Sample.

Das geladene Sample können Sie sowohl in seiner ursprünglichen Tonhöhe, als auch höher oder tiefer abspielen, je nachdem, welche Noten Sie in der MIDI-Spur programmieren. Als Vorhörfunktion dient die kleine Piano-Leiste im unteren Bereich. Die blau unterlegte Note C4 gibt das Sample in seiner Original-Tonhöhe wieder.

Sind alle gewünschten Samples für die drei MIDI-Spuren geladen, können Sie die ersten Noten programmieren. Dazu wechseln Sie in die Edit-Ansicht und wählen das Zeichenwerkzeug mit dem Stiftsymbol aus. Zeichnen Sie mit gedrückter Maustaste je einen vier Takte langen Block („Take“) in jede der drei MIDI-Spuren. Anschließend vergrößern Sie die MIDI-Spuren so, dass Sie bequem Noten eingeben können. Aktivieren Sie die Funktion „Einrasten“ und setzen Sie die Rasterauflösung auf 1/16. Durch einfaches Klicken innerhalb des Blocks setzen Sie die



Im Zeichenmodus programmieren Sie mit der Maus Noten in eine MIDI-Spur. Sie erzeugen einen Beat oder eine Melodie, indem Sie per Klick die Noten auf dem Raster platzieren.

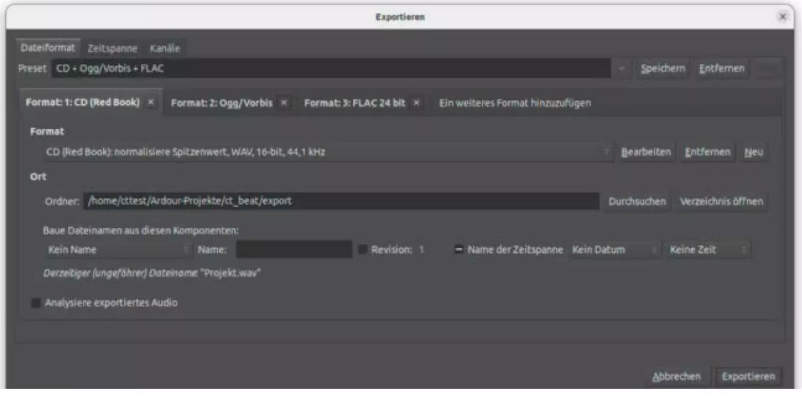
Für eine gute Aufnahme ist der richtige Pegel wichtig. Das Signal in der oberen Spur ist deutlich zu laut, in der unteren zu leise. Genau richtig ist der Pegel in der mittleren Tonspur.

Noten. An dieser Stelle ist Ihre Kreativität gefordert, jedoch gilt die oft zitierte Weisheit: Weniger ist mehr. Andere Instrumente sollen schließlich auch zur Geltung kommen.

Ein Instrument einspielen

Natürlich können Sie an dieser Stelle andere Sampler oder Software-Synthesizer laden und nach dem-

Der kostenlose Sampler samplv1 bietet viele Stellschrauben, um ein Originalsample zu bearbeiten. Von kleineren Anpassungen bis zu radikalen Verfremdungen des Originalsamples ist alles möglich.



Über die Export-Einstellungen lässt sich der fertige Song in einem Rutsch in mehrere Ausgabeformate abmischen.

selben Muster programmieren. Durch ein live eingespieltes Instrument – etwa einen E-Bass – hauchen Sie dem Beat etwas mehr Leben ein. Erstellen Sie dazu eine Audiospur, und zwar auf dieselbe Weise, wie Sie das bereits mit der MIDI-Spur getan haben. Nur wählen Sie in diesem Fall im Bereich „Vorlage/Typ“ einfach „Audio“ aus.

Den richtigen Audioeingang für die Spur wählen Sie, indem Sie mit einem Rechtsklick auf den Spurnamen das Untermenü „Eingänge“ auswählen. Dort stehen alle verfügbaren Eingänge zur Auswahl. Die Kanäle Ihres Audio-Interfaces finden Sie unter „Hardware“. Bevor Sie den roten Recording-Button aktivieren und mit der Aufnahme starten, müssen Sie Ihr Instrument zunächst einpegeln.

Der richtige Aufnahmepegel

Eine Aufnahme von Instrumenten oder einer Stimme ist simpel und schwierig zugleich. Auf der einen Seite sollte das Signal kräftig genug sein, um sich gegen andere Instrumente durchzusetzen, auf der anderen Seite aber nicht so laut, dass jegliche Dynamik während der Aufnahme verloren geht. Eins gilt es allerdings in jedem Fall zu vermeiden: digitale Verzerrungen. Diese entstehen, wenn der Eingangspegel am Input-Regler des Audio-Interfaces so hoch eingestellt ist, dass er über 0 dB hinausgeht. Laute Pegelspitzen werden abgeschnitten und machen sich als unangenehm kratzende Nebengeräusche bemerkbar. Für „fix it in the mix“ ist es dann zu spät.

Besser also von vornherein den Eingangspegel am Regler des Audio-Interfaces so einstellen, dass er weder zu leise noch zu stark ist. Da die Aufnahmen mit 24 Bit oder sogar 32 Bit gesampelt werden, sollten Sie in den Spitzen 12 dB Luft nach oben lassen. Ideal ist es, wenn die Pegelanzeige um einen Wert von -18 dB tanzt – dann haben Sie später genügend Luft für weitere Effekte im Mix. In der Mix-Ansicht können Sie den Pegel ablesen. Es empfiehlt sich, probeweise die lauteste Passage des Songs aufzunehmen, damit es dann mitten in der Aufnahme keine bösen Überraschungen gibt.

Auf diese Weise nehmen Sie Spur für Spur auf. Alle Spuren, bei denen der rote Recording-Button nicht aktiviert ist, fungieren als Playback-Spuren, das heißt, sie werden während der Aufnahme abgespielt, jedoch nicht aufgenommen. Stellen Sie nach Bedarf einzelne Instrumente zur Orientierung lauter oder leiser, um sich besser auf die Aufnahme konzentrieren zu können. Im finalen Mix regelt man die Lautstärke der Instrumente ohnehin neu.

Ein kleiner Tipp fürs Einsingen: Die Faustregel, immer circa zwei Hände breit vor dem Mikrofon zu bleiben, erspart Ihnen im Mixing-Prozess Kopfschmerzen. Durch diese Methode wird der Nahbesprechungseffekt vermieden: Je näher man an das Mikrofon herantritt, um so basslastiger wird die Stimme. Variiert der Abstand während einer Aufnahmesession permanent, gerät das Frequenzbild der Stimme durcheinander und macht im Nachhinein einen konsistenten Mix unmöglich.

DAW-Alternativen für Linux

Wenn es um Funktionen oder den Workflow von Programmen geht, lohnt es sich durchaus, mehrere Anwendungen auszuprobieren. Einige Entwickler weit verbreiteter Programme unter macOS und Windows haben den Sprung ins Linux-Ökosystem gewagt.

Reaper, eine Ardour nicht unähnliche DAW mit einem enormen Funktionsumfang und einer großen, aktiven Community, ist seit dem Release der Version 5.93 nativ für Linux verfügbar. Reaper kostet für den privaten Gebrauch oder kleinere kommerzielle Projekte 60 US-Dollar. Podcaster können das kostenlose Addon **Ultraschall 5** laden.

Wer einen Loop-basierten Workflow bevorzugt oder in der elektronischen Musik beheimatet ist, wird eher mit **Bitwig Studio** glücklich. Das nach dem Vorbild von Ableton Live gestaltete Programm bringt eine Handvoll Software-Synthesizer und viele interne Effekte mit. Die Einsteigerversion ist bereits für 99 Euro zu haben.

Ebenfalls von Ableton Live inspiriert, aber kostenlos, ist die DAW **Waveform Free** aus dem Hause Tracktion. Zwar gibt es hier eine kostenpflichtige Pro-Version, aber schon Waveform Free hat einiges zu bieten und läuft dank der ressourcenschonenden Programmierung sogar auf einem Raspi.

Freunden von Trackern wie Scream Tracker und ähnlichen Programmen aus der Demoszene der 80er und 90er Jahre sei **Renoise** ans Herz gelegt. Die etwas nostalgisch anmutende Programmierung der Notensequenzen, die aus Spalten von Hexadezimalzahlen bestehen, weckt den inneren Nerd und bietet einen etwas anderen Zugang zur eigenen Kreativität als die bisher genannten Programme. Ein sehr potenter Sample-Editor, viele interne Effekte und die Unterstützung von externen Plug-ins werten Renoise zu einer konkurrenzfähigen, wenn auch sehr eigenständigen DAW auf. Mit 68 Euro ist sie zudem recht erschwinglich.

Erwähnenswert ist auch **MusE**, eine simple DAW mit einer schlanken Oberfläche. Das kostenlose Programm ist nur für Linux erhältlich und bietet eine rudimentäre Auswahl an Audio- und MIDI-Tools. Auf bordeigene Effekte verzichtet MusE gänzlich, sodass man seine Plug-in-Sammlung selbst zusammenstellen muss.

Aus Beat wird Song

Sind Sie mit dem Ergebnis soweit zufrieden, kann der Beat zu einem Song arrangiert werden. Durch gezieltes Weglassen oder Variieren der Parts kreiert man eine Spannungskurve, die das Publikum bei der Stange hält. Gerade am Anfang ist es ratsam, sich an den Strukturen der eigenen Lieblingssongs zu orientieren. Auf diese Weise verinnerlicht man das Songwriting seiner musikalischen Vorbilder.

Sowohl MIDI- als auch Audio-Parts können Sie einfach per Copy & Paste vervielfältigen und entsprechend im Song-Arrangement verteilen. Ein wichtiges Werkzeug ist hierbei das Schneide-Tool. Dessen Scherensymbol ist als eben solches zu verstehen – setzen Sie es einfach an gewünschter Stelle an und

Platzieren Sie den Calf-Equalizer auf einer Tonspur, um dort bestimmte Frequenzen anzuheben, abzusenken oder ganz herauszufiltern.

Mit einem Limiter auf dem Master-Kanal stellen Sie die finale Lautstärke des Songs ein und verhindern digitale Verzerrungen.

zerteilen Sie mit einem Klick die Passage in zwei Teile. Mit dem Greifwerkzeug (Finger) verschieben Sie Blöcke. Ziehen Sie mit dem Greifwerkzeug am Rand einen Block größer, dann kommt der abgeschnittene Part stückweise wieder hervor. MIDI-Passagen können Sie beliebig vergrößern.

Bei den MIDI-Blöcken empfiehlt es sich, die Einrastfunktion zu aktivieren, um die Parts taktgenau zuzuschneiden. Das Tool teilt den MIDI-Block in separate Objekte, die Sie anschließend beliebig kopieren und aneinanderreihen können. Bei Audiospuren – gerade beim Gesang – sollten Sie das Einrasten jedoch ausschalten. So können Sie die Schere so ansetzen, dass die Schnitte möglichst natürlich klingen. Am besten eignen sich Stellen mit kompletter Stille. Ein kleiner Tipp bei Gesangs- oder Stimmaufnahmen: Atemgeräusche am Anfang eines Wortes dürfen ruhig auf der Aufnahme bleiben – dann klingt die zusammengeschnittene Stimme am Ende natürlicher.

Nur noch der Feinschliff

Ist die Struktur Ihres Songs fertig, geht es an die Details der Audiosignale. Ein komplettes Mixing-Tutorial würde an dieser Stelle den Rahmen sprengen. Gute Mixing-Skills setzen voraus, dass man viele Monate oder gar Jahre damit verbringt, die Zusammenhänge eines guten Mixes zu verinnerlichen.

Deshalb hier nur ein paar Worte zur grundsätzlichen Vorgehensweise: Stellen Sie als Erstes die Lautstärken der einzelnen Spuren ein, sodass alle Instrumente gut zu hören sind. Die Gesamtlautstärke des Mixes sollte dabei etwa bei -18 dB liegen. Anschließend gleichen Sie mit einem Equalizer in jeder Spur Frequenzbetonungen aus. Wenn eine Spur zu dumpf klingt, können Sie den Bereich zwischen 100 und 500 Hz beispielsweise sanft absenken, und wenn der Sänger nicht durchdringt, seine Stimme etwa im Bereich von 2 kHz etwas anheben. Schließlich gleichen Sie mit einem Kompressor Lautstärkeschwankungen aus und spendieren dem Ensemble eine Prise Hall. Grundlagen zur Bedienung von Equalizer, Kompressor, Hall & Co. erklären wir in [1].

Um einen Equalizer auf einen Kanal zu platzieren, wechseln Sie in die Mix-Ansicht. Klicken Sie mit der rechten Maustaste in den Plug-in-Bereich des jeweiligen Kanals, diesmal unterhalb des

Blocks „Fader“. Aus dem erscheinenden Kontextmenü wählen Sie „Plug-in einfügen/Nach Urheber/Calf Studio Gear/Calf Equalizer 8 Band“ aus. In der Oberfläche des Equalizers legen Sie mit den Drehreglern die Frequenzbereiche fest und wie stark diese angehoben oder abgesenkt werden sollen.

Bereit für den Export

Bevor Sie Ihren Song als Audiodatei exportieren, sollten Sie die Lautstärke mit einem Limiter anheben. Dazu laden Sie einen Limiter auf die Master-Spur, indem Sie wie zuvor ein Plug-In hinzufügen, diesmal „Calf Studio Gear/Calf Limiter“. Den Regler „Output Gain“ stellen sie rechts oben auf einen Wert von -0,3 dB, um etwas Sicherheitsabstand zur 0-dB-Grenze zu lassen, wenn Sie den Song später ins MP3 oder AAC-Format konvertieren. Die Lautstärke erhöhen Sie mit dem großen Limit-Regler in der Mitte; stellen Sie ihn so ein, dass die Absenkung (Attenuation) der Anzeige unten bei den lautesten Pegelspitzen nicht mehr als 3 bis 4 dB beträgt.

Hat Ihr Mix die richtige Lautstärke, exportieren Sie den Song in eine Datei. Öffnen Sie dazu aus dem Menü „Projekt/Exportieren/Exportiere Audiodatei(en)“ oder drücken Sie die Tastenkombination Alt+E. Es öffnet sich ein Dialogfenster mit einer Vielzahl an gängigen Export-Voreinstellungen, mit denen Sie kaum etwas falsch machen können. Durch Drücken auf die Schaltfläche „Ein weiteres Format hinzufügen“ ergänzen Sie weitere Ausgabeformate. So können Sie den Song als MP3 und als WAV-Datei mit spezifischen Vorgaben diverser Streaming-Plattformen exportieren.

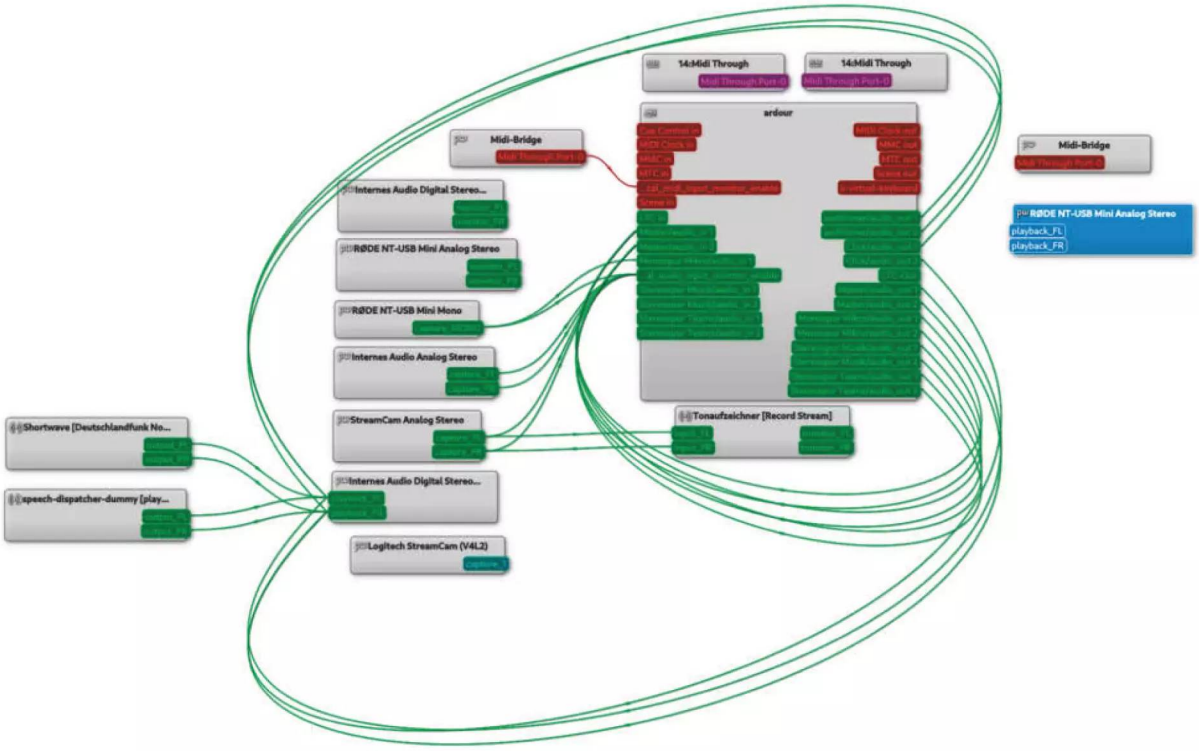
Zum Schluss noch ein Ratschlag für Recording-Einsteiger, die im Produktivitätsrausch ungeduldig dem Augenblick entgegenfiebern, den fertig gemischten Song der Öffentlichkeit zu präsentieren: Einfach noch eine Nacht drüber schlafen. Das Gehör ermüdet schneller, als einem bewusst ist. Mit frischen, ausgeruhten Ohren kann der Mix am Folgetag viel besser beurteilt werden – und so lange kann die Welt sicherlich noch auf den nächsten Hit warten. (ktn) c't

Literatur

[1] Hartmut Gieselmann, Zum Hit in 7 Tagen, Einstiegskurs: Remixen am Beispiel des Songs „Game > Over“, c't 1/2014, S. 118

Download Beispielprojekt und Samples

ct.de/wv5r



Mit WirePlumber Audiogeräte aufräumen

Wie angeschlossene Audiogeräte heißen, teilen ihre Treiber dem Betriebssystem mit – das klappt auch unter Linux. Doch nicht immer sind die Namen verständlich. Mit wenigen Kniffen passt man die Bezeichnungen systemweit an, um beim Wechsel des Mikrofons oder Lautsprechers immer das gewünschte Audiogerät zu erwischen.

Von **Keywan Tonekaboni**

Hört ihr mich jetzt?! - Die Videokonferenzsoftware hat mal wieder den falschen Audiokanal ausgewählt und die anderen Teilnehmer warten ungeduldig. Doch die Einstellungen zeigen nur unverständliche Namen: Da weiß man auf den ersten Blick gar nicht, welches Audiogerät man wählen soll. Manchmal sind auch mit der Marketingabteilung die Pferde durchgegangen: Namen wie „Tiger Lake-LP Smart Sound Technology Audio Controller“ sprengen jedes Dialogfeld. Wir zeigen, wie Sie mit einem Konfigurationsskript für den Multimedia-Sitzungsmanager WirePlumber die Namen der Audiogeräte ändern.

Bei modernen Linux-Systemen sind mehrere Komponenten für die Audiogeräte verantwortlich. Im Kernel bildet ALSA (Advanced Linux Sound Architecture) die Treiberschicht. Auf die ALSA-Schnittstellen greift ein Soundserver im Userspace zu, der als Mittler zwischen den Anwendungen und dem Treiber agiert und die parallele Nutzung desselben Audio-

kanals durch mehrere Anwendungen erlaubt. Bisher war das vor allem PulseAudio, das aber immer mehr Distributionen durch das Multimedia-Framework PipeWire ersetzen. Bei Fedora kümmert sich PipeWire schon seit Version 34 um die Audiogeräte, bei Ubuntu erst seit Version 22.10. Für ältere Versionen wie Ubuntu 22.04 LTS ist PipeWire aber in den Softwarequellen enthalten (siehe Artikel „Audioströme bequem umleiten mit PipeWire“ auf S. 56).

PipeWire bringt eine eigene PulseAudio-Implementierung mit. Daher funktionieren für PulseAudio erstellte Anwendungen auch mit PipeWire, selbst die meisten der PulseAudio-Tools. Auch die von Ubuntu Desktop und Fedora Workstation verwendete Desktopumgebung Gnome bezieht die Namen der Audiogeräte über die PulseAudio-Schnittstellen. Welcher Soundserver diese Schnittstellen bei Ihnen bereitstellt, verrät der Befehl `pactl` aus dem Paket „pulseaudio-utils“. Rufen Sie dazu in einem Terminal `pactl info` auf. Steht bei der Antwort in der Zeile „Name des Servers“ etwas von „PulseAudio (on PipeWire 0.3…)“, dann arbeitet bei Ihnen PipeWire.

WirePlumber übernimmt

Die Namen der Audiogeräte bezieht PipeWire von ALSA, das diese wiederum über Geräte-IDs, Treiber-Daten und kaum durchsichtigen Konfigurationen bildet. Damit müssen Sie sich aber nicht befassen. Um die Soundgeräte umzubenennen, benötigen Sie nur ein kleines Skript für WirePlumber. Dieser Session-Manager für PipeWire verwaltet die Verbindungen zwischen Geräten und Anwendungen und lädt die dafür benötigten Komponenten. Um die Benennung der Geräte dauerhaft festzuschreiben, hinterlegt man dazu Regeln in einer Konfigurationsdatei. Die verfasst man derzeit noch in der Programmiersprache Lua. Ab der noch unveröffentlichten Version 0.5 wechselt WirePlumber von Lua zu JSON.

Ubuntu installiert als Session-Manager standardmäßig „PipeWire Media Session“ (pipewire-media-session), der aber als veraltet gilt. Installieren Sie stattdessen WirePlumber über die Paketquellen, etwa im Terminal mit dem folgenden Befehl:

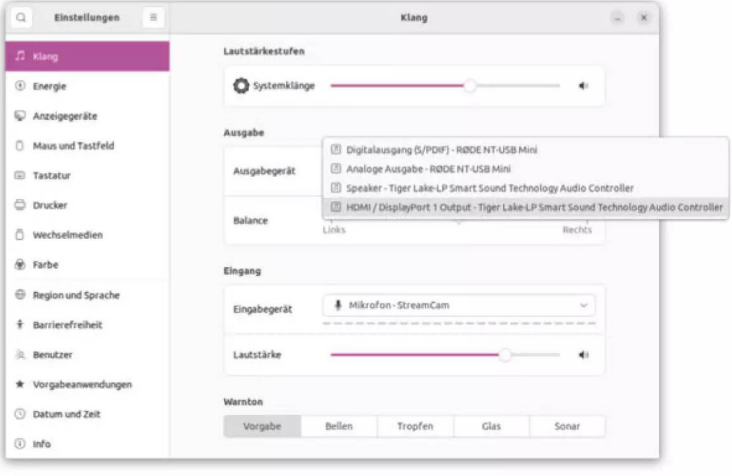
```
sudo apt install wireplumber
```

WirePlumber läuft als Systemd-User-Dienst. Die persönliche Konfiguration kann man im Homeverzeichnis festlegen (~/.config/wireplumber), muss man aber nicht. Was dort nicht festgelegt ist, holt sich WirePlumber aus den Verzeichnissen /etc/wireplumber (falls vorhanden) und /usr/share/wireplumber.

Erzeugen Sie zunächst in Ihrem Homeverzeichnis die benötigten Unterordner.

```
mkdir -p ~/.config/wireplumber/main.lua.d/
```

Legen Sie in diesem Verzeichnis eine Textdatei mit dem Namen „51-alsa-rename.lua“ an und öffnen Sie diese mit einem einfachen Texteditor wie Gedit oder dem Gnome Texteditor (gnome-text-editor).



Unnötig lange Namen von Audiogeräten sprengen den Einstellungsdialog.

Lua-Skript schreiben

Die Lua-Syntax ist etwas gewöhnungsbedürftig. Achten Sie unbedingt darauf, alle geöffneten Klammern wieder zu schließen, und Überlappungen verschiedener Klammertypen zu vermeiden. Die Grundidee besteht darin eine Regel zu formulieren, die das gewünschte Gerät anhand einer Bezeichnung identifiziert (`matches`) und ihm dann eine Eigenschaft zuweist (`apply_properties`).

```
meineregel = {
  matches = {
    {
      {
        --[[ Vergleich --]]
        "foo.bar", "equals", "pci-0000:…"
      },
    },
```

```
  },
  apply_properties = { ["KEY"] = "WERT" }
}
```

Die scheinbar überflüssigen Klammern bei `matches` dürfen Sie keinesfalls weglassen, da WirePlumber ein verschachteltes Array erwartet. Dadurch lassen sich mehrere Vergleiche mit Und- und Oder-Bedingungen verknüpfen, was aber hier zu weit führen würde (siehe Dokumentation unter ct.de/wazx).

Bevor Sie Regeln definieren können, benötigen Sie die Gerätebezeichnungen für den Vergleich. Öffnen Sie dazu ein Terminal und listen per `wpctl status` alle mit Ihrer PipeWire-Session verbundenen Objekte, von Anwendungen bis hin zur Hardware. Suchen Sie unter „Audio / Devices“ den Eintrag zu Ihrem Audiogerät. Die Nummer vor dem Namen ist die aktuelle ID. Verwenden Sie diese ID (zum Beispiel 32), um per `wpctl` die Eigenschaften des Gerätes anzuzeigen:

```
wpctl inspect 32
```

Kopieren Sie für PCI-Geräte wie die Onboard-Soundkarte den Wert hinter „device.bus-path“ und bei USB-Geräten den Wert bei „device.bus-id“. Dieses Wertepaar tragen Sie nun in der Konfigurationsdatei als Regel ein:

```
regel = {
  matches = {
    {
      { "device.bus-path", "equals",
        "pci-0000:00:1a.3-platform-skl_hda…" },
    }
  },
  apply_properties = {
    ["device.description"] = "Internes Audio" }
}
```

Nach dem gleichen Prinzip gehen Sie innerhalb von „apply_properties“ vor und weisen dem Schlüssel „device.description“ den gewünschten Namen als Zeichenkette zu.

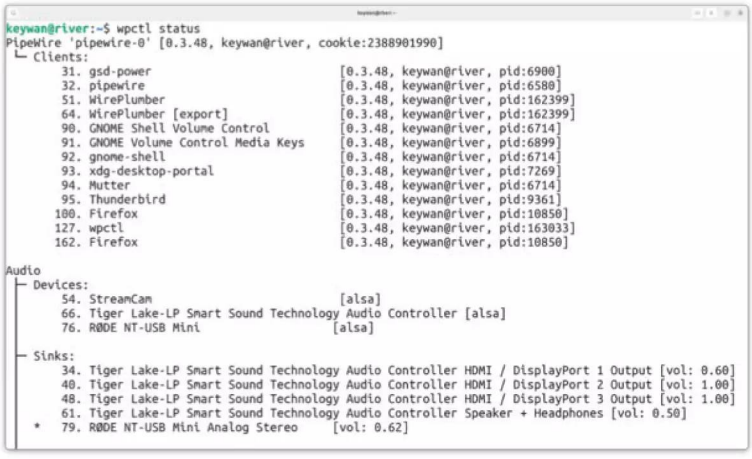
Fügen Sie diese Regeln nun der dafür vorgesehenen Tabelle „alsa_monitors.rules“ hinzu. Ergänzen Sie dafür die Konfiguration am Ende um folgende Zeile:

```
table.insert(alsa_monitor.rules,regel)
```

Speichern Sie die Datei ab. Um die Regeln anzuwenden, starten Sie WirePlumber neu, indem Sie `systemctl --user restart wireplumber.service` im Terminal eingeben. Öffnen Sie anschließend in Gnome die Systemeinstellungen und kontrollieren Sie im Abschnitt Klang die Bezeichnungen der Audiogeräte. Greifen die Regeln, erscheint dort der geänderte Name.

Sollte dort kein Audiogerät auftauchen, haben Sie vermutlich einen Syntaxfehler in Ihrer Konfigurationsdatei. Kontrollieren Sie Klammern und Kommata. Beobachten Sie in einem separaten Terminalfenster mit `journalctl -f --user -u wireplumber`, ob WirePlumber einen Fehlstart meldet, wenn Sie den Dienst neu starten.

Um Ihnen etwas Kopfzerbrechen zu ersparen, stellen wir unter ct.de/wazx eine Vorlage des Lua-Skripts zum Download bereit.



Mit dem Befehl wpctl listet WirePlumber auf, welche Anwendungen und Geräte aktuell auf das Multimedia-Framework PipeWire zugreifen.

Wege und Grenzen

Statt exakter Vergleiche mit `equals` können Sie auch mit `matches` nach einem Muster suchen. Nutzen Sie dafür im Suchstring * als Wildcard. Mit den Schlüsselwörtern `node.description` und `device.profile.description` benennen Sie die Namen der Ein- und Ausgänge („Mikrofon“, „HDMI / DisplayPort Output“). Leider übernimmt Gnome die Werte nicht, sondern fragt die Namen der Kanäle über andere Felder ab, die sich ohne Weiteres nicht ändern lassen. PipeWire-Anwendungen wie qpwgraph hingegen zeigen auch diese Namen korrekt an. (ktn) **ct**

Beispielkonfiguration zum Download und Dokumentation

ct.de/wazx

Do KI Yourself!

Modelle anwenden und selbermachen

Heft + PDF mit 29 % Rabatt

Was muss man technisch über KI wissen? Damit beschäftigt sich dieses iX-Special und hat für jeden Wissensstand etwas im Gepäck. Erfahrene Entwickler finden Tipps zu fertigen KI-Modellen und Quellen von Trainingsdaten; Anfänger und Interessierte holt das Heft bei bei der Architektur von Sprachmodellen und der Funktionsweise von KI-Bildgeneratoren ab. Für alle dazwischen bietet das Special Informationen, um aktuell wirklich mitreden zu können:

- ► Was große KI-Modelle können: So funktionieren GPT-4, Bard, Stable Diffusion und Co.
- ► Mit PyTorch und scikit-learn in die KI-Entwicklung starten
- ► Mit LangChain KI-Agenten bauen und eigene Daten nutzen
- ► Neuronale Suche: Finden, was wirklich gemeint ist
- ► Aktuelle GPUs im Leistungsvergleich
- ► KI und Recht: Urheberrecht, DSGVO, Data Act und AI Act
- ► Auch als Angebots-Paket Heft + PDF + Buch "Natural Language Processing mit Transformern" erhältlich!

Heft für 14,90 € • PDF für 14,90 € • Bundle Heft + PDF 20,90 €

shop.heise.de/ix-ki

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 € (innerhalb Deutschlands). Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

heise Shop

Mit Udev Zugriffsrechte gewähren

Die Alleinherrschaft über den eigenen USB-Stick? Oder die Maustasten für jedes Spiel individuell neu belegen? Kein Problem für Udev, den Daemon für Hardware-Events unter Linux. Mit ausgefeilten Udev-Regeln erleichtern Sie sich den Linux-Alltag.

Von **Mirko Dölle**

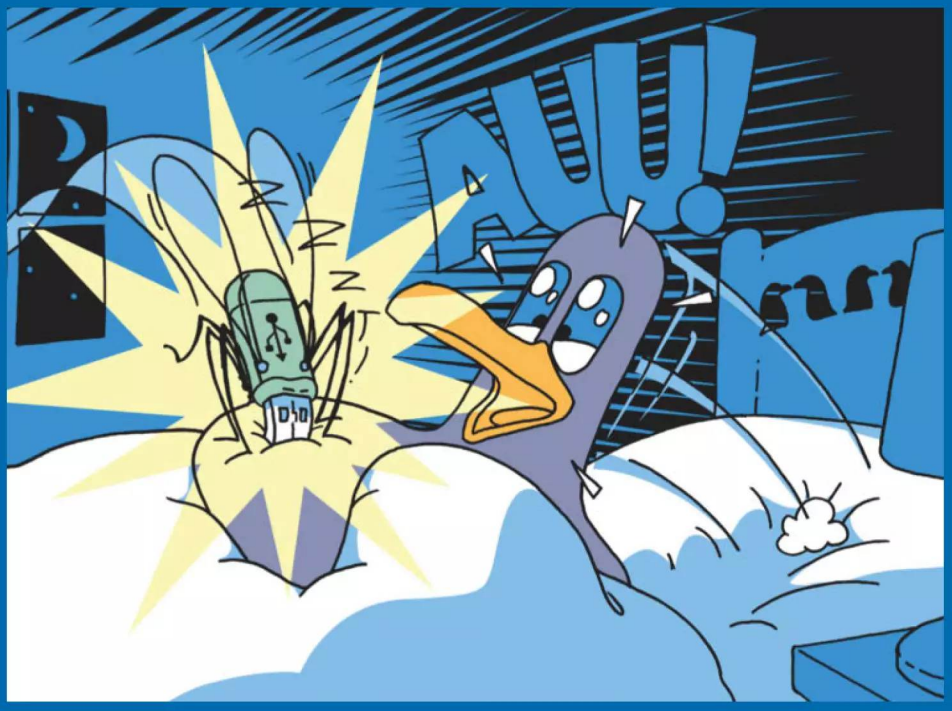


Bild: Rudolf A. Blaha

Erkennt Linux ein neues USB-Gerät, übernimmt der Daemon Udev mit seinem komplexen Regelwerk die Initialisierung der Hardware, spielt Firmware auf und legt Gerätedateien an. Indem Sie Ihre eigenen Regeln einfügen, können Sie im Alltag auch ohne Root-Rechte Ihren USB-Stick mit neuen Linux-Distributionen bespielen oder Hardware individuell konfigurieren, damit die Gaming-Maus die gewünschte Tastenbelegung für Ihr Lieblingsspiel hat.

Die Aufgabe des Udev-Daemon ist, vom Kernel festgestellte Hardware-Veränderungen nach einem Regelwerk zu verarbeiten – also immer dann tätig zu werden, wenn etwa ein USB-Gerät angeschlossen oder auch eine Festplatte aus dem Wechselrahmen entfernt wird. Die meisten der über 100 vorinstallierten Regeln verändern die Zugriffsrechte auf die vom Kernel erkannte Hardware und kümmern sich etwa darum, dass Benutzer ohne Root-Rechte auf DVD-Laufwerke, USB-Sticks oder Modems zugreifen dürfen oder dass CD- und DVD-Laufwerke unabhängig vom konkreten Typ stets unter dem symbolischen Link /dev/cdrom erreichbar sind. Die prominentesten Regeln jedoch sind jene, die dem Sound-System des Desktops Zugriff auf die Soundkarte verschaffen – ohne sie bliebe der Desktop stumm.

Die meisten der standardmäßig unter /usr/lib/udev/rules.d gespeicherten Regeln werden beim Booten abgearbeitet, wenn der Kernel die einzelnen Systembusse nach Geräten scannt und dann an den Udev-Daemon meldet. Ändern sollten Sie diese Regeldateien nicht, denn sie würden bei einem Update von Udev überschrieben. Stattdessen legen Sie bei Bedarf eine neue Datei im Verzeichnis /etc/udev/rules.d an, die als Dateiendung `.rules` im Namen tragen muss. Udev vermischt den Inhalt beider Verzeichnisse und arbeitet die Regeldateien in lexikografischer Reihenfolge ab – die Regeln aus /usr/lib/udev/rules.d/50-firmware.rules werden also vor denen aus der Datei /etc/udev/rules.d/70-persistent-net.rules verarbeitet; haben zwei Dateien den gleichen Namen, so kommt die aus /usr/lib/udev/rules.d zuerst dran.

Die Regeldateien liegen im Textformat vor und lassen sich leicht lesen. Folgendes zeigt einen Auszug aus der Datei /etc/udev/rules.d/70-persistent-net.rules einer openSUSE-Installation:

```
# PCI device 0x10ec:0x8168 (r8169)
SUBSYSTEM=="net", ACTION=="add", ↴
↳DRIVERS=="?*", ↴
↳ATTR{address}=="f8:a9:63:48:d4:7a", ↴
↳ATTR{dev_id}=="0x0",↴
↳ATTR{type}=="1", ↴
↳KERNEL=="eth*", NAME="eth0"
```

Kommentarzeilen beginnen wie auch bei anderen Programmen üblich mit einem Doppelkreuz. Alle anderen Zeilen sind Udev-Regeln, die jeweils aus Bedingungen und Zuweisungen bestehen. Der Unterschied ist einfach: Die Operatoren `==` und `!=` stehen für Vergleiche, Zuweisungen sind `=`, `+=`, `-=` und `:=` – letzteres bedeutet, dass die Zuweisung final ist und durch keine weitere Regel mehr verändert werden darf.

Feine Unterschiede

Die Regel aus dem Beispiel bezieht sich auf das Netzwerk (`SUBSYSTEM=="net"`) und gilt nur, wenn ein Gerät hinzugefügt wird (`ACTION=="add"`). Deutlich zu erkennen: Zeichenketten müssen stets von Anführungszeichen eingeschlossen sein. Die einzelnen Bestandteile einer Regel sind über Kommas miteinander verknüpft. Auch Wildcards sind erlaubt, bei `DRIVERS=="?*"` zum Beispiel steht das Fragezeichen für ein beliebiges einzelnes Zeichen, der Stern dahinter für beliebig viele weitere Zeichen. In der Kombination bedeutet `"?*"`, dass das Feld nicht leer sein darf (darauf würde `"*"` nämlich auch passen), der Name des Treibers aber beliebig ist.

Der wichtigste Teil der Regel ist `ATTR{address}` gefolgt von einer Ethernet-MAC-Adresse: Die Regel gilt also nur für ein Gerät, das ein Attribut `address` mit der genannten MAC-Adresse hat. Da MAC-Adressen von Netzwerkadaptern für jedes einzelne Gerät individuell vergeben werden, passt die Regel auch nicht auf einen anderen Netzwerkadapter desselben Herstellers und Modells. Was die Regel bewirkt, steht ganz am Ende: `NAME="eth0"` legt den Gerätenamen fest und sorgt dafür, dass dieser eine Netzwerkadapter mit der angegebenen MAC-Adresse stets den Namen `eth0` erhält. Schließen Sie einen anderen Netzwerkadapter an, so bekommt dieser einen anderen Namen. So ist sichergestellt, dass bei Rechnern mit zwei Ethernet-Anschlüssen nicht versehentlich die Ports vertauscht werden und plötzlich interne Dienste von außerhalb erreichbar sind.

Änderungen an Regeldateien sollte Udev übrigens automatisch erkennen und unmittelbar berücksichtigen. Sollte dies einmal nicht klappen, müssen Sie dafür nicht neu booten, sondern können Udev veranlassen, sämtliche Regeldateien neu zu laden:

```
sudo udevadm control --reload-rules
```

Magischer Stick

Während sich USB-Ethernet-Adapter anhand der herstellerübergreifend weltweit eindeutigen MAC-Adresse zuverlässig identifizieren lassen, gibt es bei USB-Sticks nur die Seriennummer – und die vergibt jeder Hersteller nach eigenem Gusto. Damit Sie die Alleinherrschaft über Ihren USB-Stick bekommen und ihn zum Beispiel auch ohne Root-Rechte und `sudo` mit einer neuen Linux-Distribution bespielen dürfen, müssen Sie neben der Seriennummer auch unbedingt Vendor- und Product-ID überprüfen, damit Sie nicht versehentlich den falschen Stick überschreiben. Diese und viele andere Daten eines USB-Geräts erhalten Sie von `udevadm`, hier ein Beispielaufruf:

```
sudo udevadm info --attribute-walk /dev/sdb
```

`udevadm` erwartet als Gerätenamen den SysFS-Gerätepfad. Geben Sie hingegen einen Gerätenamen aus /dev an, versucht udevadm automatisch, diesen in einen SysFS-Gerätepfad umzuwandeln, was aber nicht immer klappt. Wie Sie bei Bedarf den SysFS-Gerätepfad herausfinden, wird noch später erklärt, für den Moment genügt es, wenn Sie den Gerätenamen an den Ihres USB-Sticks anpassen, wobei Ihnen das Kommando `lsblk` hilft.

Der `--attribute-walk` bewirkt, dass sich `udevadm` im Gerätepfad des SysFS Stück für Stück nach oben vorarbeitet und auch die Daten der Elterngeräte wie zum Beispiel die des USB-Controllers, an dem der Stick angeschlossen ist, anzeigt. Die Liste der Geräteeigenschaften und vor allem der Udev-Attribute ist sehr lang. Was die einzelnen Attribute bedeuten, lässt sich anhand des Namens meist leicht ermitteln. Hier ein Auszug mit den relevanten Daten eines USB-Sticks von Silicon Motion:

```
ATTRS{idVendor}=="090c" ↴
ATTRS{idProduct}=="1000"
ATTRS{serial}=="9211070000002703"
```

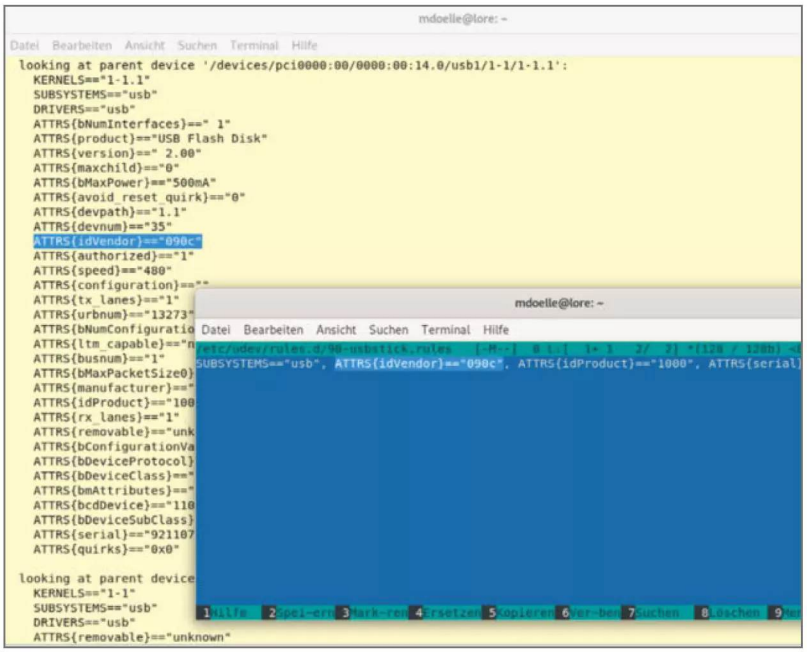
Der Anfang der Udev-Regel für diesen USB-Stick lautet somit

```
SUBSYSTEMS=="usb", ↴
↳ATTRS{idVendor}=="090c", ↴
↳ATTRS{idProduct}=="1000", ↴
↳ATTRS{serial}=="9211070000002703"
```

Damit ein bestimmter Benutzer die vollen Zugriffsrechte auf diesen speziellen USB-Stick erhält und dort ohne Root-Rechte Linux-Distributionen aufspielen darf, weisen Sie ihn als Eigentümer aus:

```
OWNER="mdoelle"
```

Vergessen Sie nicht das Komma zwischen der bisherigen Regel und der Erweiterung.



Copy & Paste statt Handarbeit: Das Verwaltungsprogramm udevadm gibt die Udev-Attribute von Geräten genau so aus, wie Sie sie in Regeldateien eintragen müssen.

Umgebungsvariablen

Damit der Automounter des Desktops den Stick ignoriert, schließlich dient er ja nur zum Ausprobieren neuer Linux-Distributionen, können Sie die Umgebungsvariable `UDISKS_IGNORE` setzen:

```
ENV{UDISKS_IGNORE}="1"
```

Diese Variable ist auch praktisch, wenn Sie die Systempartition eines parallel installierten Windows im Dateimanager des Desktops ausblenden wollen. Eine Übersicht aller nutzbaren Umgebungsvariablen gibt es nicht, denn wie im Fall von `UDISKS_IGNORE`

Logitech G300s mit Ratslap konfigurieren

Damit das Startskript eines Spiels die Tastenbelegung der Gaming-Maus automatisch anpassen kann, eignet sich `ratslap` – denn anders als das grafische Tool Piper können Sie die neue Tastenbelegung bei `ratslap` mittels Kommandozeilenparametern konfigurieren. Die Quellen von `ratslap` finden Sie auf GitLab. Als einzige Voraussetzung, um das Programm übersetzen zu können, müssen die Standard-Entwicklungswerkzeuge installiert sein, unter Debian und Ubuntu sind das die Pakete `git` und `build-essential`:

```
sudo apt install git build-essential
```

Das Git-Repository von `ratslap` laden Sie mit folgenden Befehlen herunter und übersetzen die Quellen:

```
git clone \
 https://gitlab.com/krayon/ratslap.git
cd ratslap
make
```

Damit `ratslap` allen Benutzern zur Verfügung steht und ohne `sudo` aufgerufen werden kann, installieren Sie es im Verzeichnis /usr/local/bin, ändern die Gruppe auf `input` und setzen das SGID-Bit, sodass `ratslap` stets mit den Rechten dieser Gruppe startet:

```
sudo cp ratslap /usr/local/bin/
sudo chgrp input \
  /usr/local/bin/ratslap
sudo chmod g+s /usr/local/bin/ratslap
sudo cp manpage.1 \
  /usr/local/man/man1/ratslap.1
```

Die Manual Page (`man ratslap`) beschreibt, wie Sie zwischen den drei Profilen der Logitech G300s umschalten, die Auflösung anpassen, die Tastenbelegung auslesen und verändern. Wenn Sie die im Artikel beschriebene Udev-Regel nutzen, damit das USB-Device zur Gruppe `input` gehört, klappt das sogar ohne Root-Rechte respektive `sudo`. Mit dem folgenden Kommando schalten Sie auf das zweite Profil (`f4`) um und belegen die fünfte Sondertaste des Profils mit der Taste 1 des Ziffernblocks, um damit in 7 Days to Die auf die erste Waffe am Werkzeuggürtel zu wechseln:

```
ratslap -s f4 -m f4 -5 Num1
```

gelten sie oft für nachgelagerte Dienste oder Programme. Welche Udev-Umgebungsvariablen auf Ihrem System bereits in Gebrauch sind, können Sie mit folgendem Befehl ermitteln:

```
grep -hro 'ENV{[^}]*}=\+[^,]*' ↵
↳/{usr/lib,etc}/udev/rules.d | sort -u
```

Wohlgemerkt werden nur jene Umgebungsvariablen angezeigt, die bereits in einer Udev-Regel erwähnt werden, egal ob als Abhängigkeit oder als Zuweisung. Indem Sie eine Volltextsuche in den Manpages Ihres Systems nach den vorgefundenen Umgebungsvariablen starten, finden Sie oft die Quelle und dann auch weitere Optionen – im Fall von `UDISKS_IGNORE` mit dem Befehl

```
man -K -I UDISKS_IGNORE
```

Etliche Umgebungsvariablen setzt Udev allerdings selbst, nicht zuletzt, damit man sie in Regeln, aber auch in nachgelagerten Programmen und Diensten wie systemd verwenden kann. Welche das sind, finden Sie am leichtesten heraus, indem Sie erst im Terminal `sudo udevadm monitor --env` aufrufen und dann das USB-Gerät anschließen.

Event-Monitoring

Der Monitor-Modus von `udevadm` ist auch praktisch, wenn Sie den Gerätenamen des neu angeschlossenen Geräts nicht kennen oder ihn partout nicht finden. Das kann leicht bei Mäusen und Tastaturen passieren, wo man dann unter einem Dutzend Eingabegeräten das richtige heraussuchen müsste, aber auch bei Entwicklungsplatinen wie dem Arduino, die als USB-Gerät programmiert sind oder zu denen man eine serielle Verbindung herstellen möchte, etwa um Log-Daten auslesen zu können.

Als Beispiel dient nachfolgend die Gaming-Maus G300s von Logitech mit sechs frei belegbaren Sondertasten. Anstatt vor jedem Spiel mit dem grafischen Maus-Tool Piper die Tastenbelegung zu verändern, können Sie das Konfigurationsprogramm `ratslap` von GitLab [1] verwenden und so Profil und Tastenbelegung aus dem Startskript des Spiels heraus individuell anpassen. Dazu benötigt `ratslap` allerdings Zugriff auf das USB-Device, das standardmäßig Root gehört. Sie müssten daher `sudo` für den Aufruf von `ratslap` verwenden und müssten das Spiel im Terminal aufrufen, um das Passwort einzugeben.

Gruppenzwang

Die bessere Alternative ist, `ratslap` der Gruppe `input` zuzuordnen, die üblicherweise Zugriff auf Eingabegeräte hat, und das Programm mit dem SGID-Flag zu versehen (siehe Kasten „Logitech G300s mit Ratslap konfigurieren“). Damit auch das USB-Device künftig der Gruppe `input` gehört, müssen Sie Udev anweisen, die Gruppenzugehörigkeit nach dem Anschließen zu ändern. Die Attribute für die Udev-Regel ermitteln Sie wiederum mit `udevadm` – allerdings müssen Sie dafür den Gerätepfad der Maus herausfinden. Dabei hilft ein Blick in die System-Logs, entweder mit dem Befehl `sudo dmesg | less` oder `sudo less /var/log/syslog`. Suchen Sie dort nach einem Hinweis auf den Hersteller. Die Suchfunktion in `less` öffnen Sie mit dem Schrägstrich, dahinter geben Sie den Suchbegriff ein – also in diesem Fall `/Logitech`. Dort finden Sie in den Meldungen des Treibers auch den Gerätepfad; die Log-Meldung sieht etwa wie folgt aus:

```
input: Logitech G300s Optical Gaming↴
↳ Mouse as /devices/pci0000:00↴
↳/0000:00:08.1/0000:0c:00.3/usb5/5-4↴
↳/5-4:1.0/0003:046D:C246.0004↴
↳/input/input5
```

Der dort angegebene Gerätepfad bezieht sich auf das System-Dateisystem SysFS, das unter `/sys` eingebunden ist – für einen vollständigen Pfad müssen Sie also noch `/sys` voranstellen. Die Udev-Attribute der Maus rufen Sie ab, indem Sie `udevadm` mit einem ellenlangen Pfad füttern:

```
sudo udevadm info --attribute-walk ↴
↳--path /sys/devices/pci0000:00↴
↳/0000:00:08.1/0000:0c:00.3/usb5/↴
↳5-4/5-4:1.1/0003:046D:C246.0005/↴
↳input/input7
```

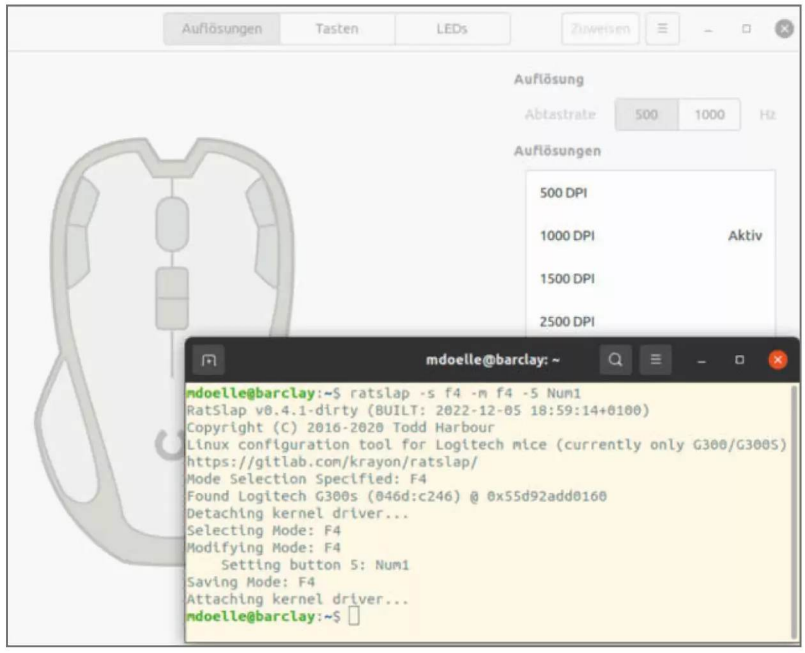
Auf diese Weise gelangen Sie wiederum an alle benötigten Udev-Attribute. Finden Sie den Gerätepfad in den Systemlogs nicht, gibt es noch eine weitere Möglichkeit: Entfernen Sie zunächst das USB-Gerät, rufen im Terminal `sudo udevadm monitor --property` auf und schließen das Gerät wieder an. Auch so erhalten Sie alle Udev-Attribute.

In den Udev-Eigenschaften finden Sie unter anderem die Vendor- und Product-ID. Seriennummer und weitere Gerätedetails sind für die Gaming-Maus nicht nötig, denn falls Sie eine andere Maus gleichen Typs anschließen, möchten Sie ja ebenfalls die Tastenbelegung verändern können – die Regel soll also für alle Logitech G300s gelten, nicht nur für dieses eine Exemplar. Dementsprechend lautet die Udev-Regel

```
SUBSYSTEMS=="usb", ATTRS{idVendor}==↴
↳"046d", ATTRS{idProduct}=="c246", ↴
↳GROUP="input"
```

Geht es nur um die Vendor- und Product-ID eines USB-Geräts, so können Sie statt `udevadm` auch `lsusb` konsultieren, das alle angeschlossenen USB-Geräte auflistet. Hier finden Sie ebenfalls beide Angaben, durch Doppelpunkt getrennt:

```
Bus 005 Device 003: ID 046d:c246 ↴
↳Logitech, Inc. Gaming Mouse G300
```



Mit `ratslap` können Sie die Sondertasten der Gaming-Maus Logitech G300s für jedes Spiel individuell aus dessen Startskript heraus anpassen. Beim grafischen Maus-Tool Piper müssten Sie das von Hand erledigen.

Fazit

Mit `udevadm` können Sie per Copy & Paste Ihre eigenen Udev-Regeln zusammenstellen, statt sie aufwendig und fehlerträchtig von Hand zu schreiben. Richtig angewendet, ersparen Sie sich im Alltag an vielen Stellen die Eingabe des Root-Passworts und können leicht unterschiedliche Netzwerkumgebungen im Büro und im Homeoffice auseinanderhalten. (mid) c't

Literatur

[1] Ratslap auf GitLab: gitlab.com/krayon/ratslap

Schalten und walten mit NetworkManager

Bei vielen Linux-Desktops kümmert sich der NetworkManager-Daemon um das Netzwerk und bleibt dabei meist dezent im Hintergrund. Der Dienst führt auf Wunsch aber auch Skripte aus, sobald man das Netzwerk wechselt. Wir zeigen, wie Sie selbst so ein Skript erstellen.

Von **Keywan Tonekaboni**

Der NetworkManager-Daemon kann mehr, als dessen grafische Bedienoberflächen in Gnome, Cinnamon und anderen Linux-Desktops erahnen lassen. Im Hintergrund versucht er, automatisch eine funktionierende Netzwerkverbindung aufzubauen, ganz gleich, ob über LAN, WLAN oder VPN. NetworkManager hat mit dem Dispatcher zudem einen Dienst, der bei Veränderungen an der Netzwerkverbindung vom Benutzer hinterlegte Skripte ausführt. Damit können Sie zum Beispiel automatisch eine Netzwerkfreigabe mounten, sobald Sie Ihren Laptop mit dem heimischen Netz verbinden. Oder schonen Sie den Akku, indem Sie die WLAN-Schnittstelle ausschalten, sobald Sie ein Netzwerkkabel einstecken. Wir zeigen, was es dabei zu beachten gilt und wie Sie selbst ein Skript erstellen.

Arbeitsweise

NetworkManager durchsucht die Verzeichnisse /etc/NetworkManager/dispatcher.d und /usr/lib/NetworkManager/dispatcher.d und führt die dort vorhandenen ausführbaren Skripte nacheinander in lexikografischer Reihenfolge aus. Da /usr/lib für Distributionsskripte vorgesehen ist, speichern Sie unterhalb von /etc/NetworkManager/dispatcher.d Ihre eigenen Skripte, damit diese bei Updates nicht überschrieben oder gelöscht werden. Das Skript muss dem User root gehören und nur er darf dafür Schreibrechte haben, sonst ignoriert NetworkManager es.

Beim Aufruf übergibt NetworkManager zwei Argumente an die Skripte: den Namen der Netzwerkschnittstelle („enx…“, „tun1“ …), gefolgt vom auslösenden Ereignis (up, down, dhcp4-change …), auch Aktion genannt. Mögliche Werte sind in der Tabelle NetworkManager-Aktionen aufgeführt. Bei Verbindungen, die VPN-Plug-ins aufbauen, ist den Aktionsnamen ein „vpn-“ vorangestellt (vpn-up, vpn-pre-down …). Das gilt aber nicht für WireGuard-Verbindungen.

NetworkManager-Aktionen

Aktion	Beschreibung
up/down	Netzwerkschnittstelle wurde aktiviert/deaktiviert.
pre-up	Aktivierung der Netzwerkschnittstelle wird vorbereitet.
pre-down	Deaktivierung der Netzwerkschnittstelle wird vorbereitet.
hostname	Hostname wurde geändert.
dhcp4-change/dhcp6-change	DHCP-Lease hat sich geändert (IPv4/IPv6).
connectivity-change	Verbindungsstatus hat sich geändert (online, limitiert, offline).

Die Aktionen pre-up/pre-down werden nur ausgeführt, wenn NetworkManager selbst die Netzwerkschnittstelle aktiviert oder deaktiviert. Ziehen Sie beispielsweise das Netzwerkkabel ab, hat NetworkManager keine Gelegenheit mehr, pre-down aufzurufen. Zudem werden nur Skripte ausgeführt, die in den Unterordnern pre-up.d respektive pre-down.d vorhanden sind. Es reicht aber aus, ein in dispatcher.d vorhandenes Skript zu verlinken.

Einen Sonderfall bilden die Aktionen hostname und connectivity-change, die als Schnittstellennamen „none“ oder ein leeres Feld übergeben.

Skript erstellen

Das Beispielskript (siehe unten) soll die WLAN-Schnittstelle bei Anschluss eines LAN-Kabels deaktivieren, um Strom zu sparen. Zeile 2 weist die übergebenen Argumente den Variablen `$IFACE` und `$EVENT` zu, um die Lesbarkeit zu erhöhen. Die Parameter `$1` und `$2` stehen in Anführungszeichen, damit ein leeres Feld wie bei connectivity-change keine Fehler verursacht. Um die Fehlersuche zu erleichtern, schreibt `logger` Angaben zum Dispatcher-Aufruf in den Systemlog. Die sehen Sie, wenn Sie `journalctl -f` in einem Terminalfenster aufrufen.

Neben den übergebenen Parametern gibt es weitere Umgebungsvariablen, die Sie in Ihrem Skript abrufen können. So enthält etwa `$CONNECTION_ID` den Namen der Verbindung. Eine Liste der verfügbaren Variablen verrät die Manpage, die Sie mit `man NetworkManager-dispatcher` aufrufen. Manche Variablen sind nur bei bestimmten Aktionen verfügbar, zum Beispiel `$CONNECTIVITY_STATE` bei connectivity-change.

Das Skript definiert in `$DEVICES` eine Liste der zu beobachtenden Netzwerkschnittstellen. Die Namen ermitteln Sie mit `ip link`. Wenn der vom Dispatcher übergebene Schnittstellenname in der Liste vorhanden ist, verarbeitet das Skript die Aktion. Lautet die Aktion „up“, dann deaktiviert das Kommandozeilentool `nmcli` die WLAN-Schnittstelle. Bei „down“, also deaktivierter LAN-Schnittstelle, schaltet nmcli das WLAN-Interface wieder an. Das Programm nmcli gehört zu NetworkManager.

Kopieren Sie mit Root-Rechten das fertige Skript nach /etc/NetworkManager/dispatcher.d/50-wifi-switch.sh. Wechseln Sie dann in dieses Verzeichnis und passen Sie die Dateirechte an.

```
sudo -i
cd /etc/NetworkManager/dispatcher.d/
chown root:root 50-wifi-switch.sh
chmod 755 50-wifi-switch.sh
```

Damit NetworkManager das Skript künftig ausführt, starten Sie den Dienst über Systemd neu:

```
sudo systemctl restart NetworkManager
```

Beobachten Sie mit `journalctl -f`, ob NetworkManager korrekt startet und das Skript ausführt, wenn Sie das Netzwerkkabel verbinden oder trennen.

```
01 #!/bin/bash
02 IFACE="$1"; EVENT ="$2"
03
04 # Liste der zu beobachtenden Netzwerknamen
05 DEVICES="eth0 enx1234567890AF"
06
07 # Debug-Informationen
08 logger "Netzwerk-Dispatcher: iface:$IFACE event:$EVENT" \
09        "id: $CONNECTION_ID uuid: $CONNECTION_UUID"
10
11 # Wenn $DEVICES die Zeichenkette aus $IFACE enthält, dann…
12 if [[ $DEVICES =~ $IFACE  ]]; then
13
14 # Je nach Event, WLAN an- oder ausschalten.
15 case "$EVENT" in
16   up)
17     logger "Netzwerk-Dispatcher: Schalte WLAN aus."
18     nmcli radio wifi off ;;
19   down)
20     logger "Netzwerk-Dispatcher: Schalte WLAN an."
21     nmcli radio wifi on ;;
22 esac
23 fi
```

Mit einem Shellskript für den Dispatcher-Dienst des NetworkManager schalten Sie das WLAN ab oder an, abhängig davon, ob eine Ethernet-Schnittstelle verwendet wird.

Gebrauchshinweise

Achten Sie darauf, dass Ihre Skripte zügig arbeiten. Braucht ein Skript zu lange, schießt NetworkManager es wieder ab, wobei die Manpage kein genaues Limit nennt. Sollen Skripte parallel starten, hinterlegen oder verlinken Sie diese im Unterverzeichnis no-wait.d. NetworkManager wartet allerdings nicht auf Skripte und beendet diese auch nicht, wenn es eine neue Netzwerkaktion gibt. Wenn etwa ein Skript bei Verbindung mit dem Firmennetz eine Netzwerkfreigabe mounten soll und Sie in kurzer Folge das LAN-Kabel ein- und ausstecken, versucht das Skript weiter, den Mount-Vorgang durchzuführen.

Bedenkt man diese Rahmenbedingungen, kann man sehr leicht Aktionen automatisieren, die bei Änderungen an der Netzwerkverbindung ausgeführt werden. (ktn) c't

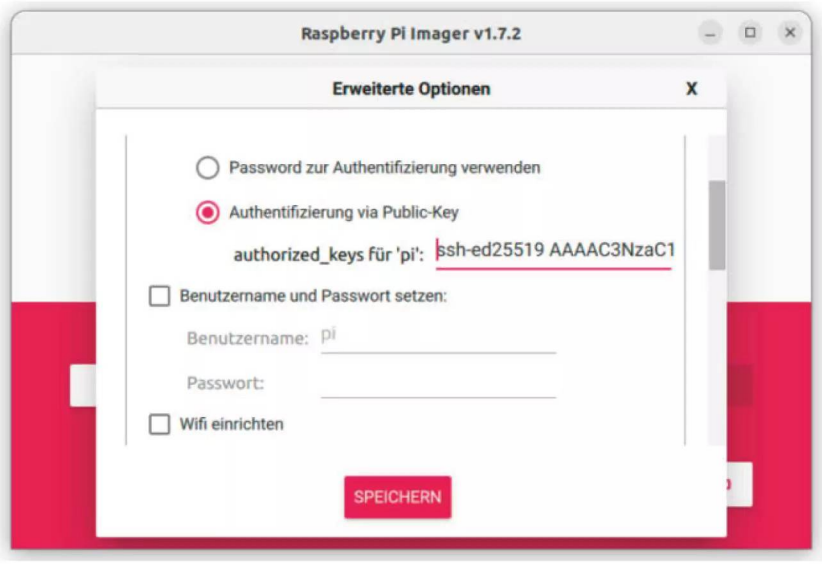
Bild: Andreas Martini

Sicher und bequem arbeiten mit SSH

Die Secure Shell (SSH) ist eines der wichtigsten Werkzeuge für alle, die beruflich oder privat Server administrieren und regelmäßig Systeme fernwarten. Mit ein paar Kniffen gestalten Sie Ihren SSH-Alltag komfortabler und nehmen Schlüssel dank FIDO2 mit auf Reisen, ohne Kompromisse bei der Sicherheit einzugehen.

Von **Niklas Dierking**

Ein typischer SSH-Verbindungsaufbau mit dem Befehl `ssh ndi@example.com` bietet etliche Gelegenheiten für Tippfehler und verlangt viel Gehirnschmalz, wenn Sie mehr als eine Handvoll Server verwalten. „In welchem Passwortmanager hatte ich doch gleich mein Root-Passwort hinterlegt?“, „Wie war nochmal die IP-Adresse meines Mietservers?“ - Administrieren per SSH kann mühselig sein. Wir erklären, wie Sie Ihren SSH-Alltag optimieren und dabei noch sicherer unterwegs sind. In diesem Artikel kommt Ubuntu 22.04 LTS als OpenSSH-Client und -Server zum Einsatz. Viele



Sie müssen öffentliche Schlüssel nicht kompliziert auf Zielsysteme kopieren, wenn Sie diese direkt bei der Einrichtung des Systems hinterlegen, etwa mit dem Raspberry Pi Imager.

Tipps lassen sich auch auf macOS oder Windows übertragen.

Der erste Schritt für mehr Sicherheit und Komfort in der Arbeit mit SSH liegt im Umstieg von Passwörtern auf Schlüsselpaare. Wenn Sie die Anmeldung mit Passwort erlauben, dann geben Sie potenziellen Eindringlingen die Chance, Benutzernamen und Passwörter durchzuprobieren. Funktioniert die Anmeldung am SSH-Server dagegen ausschließlich mit gültigem Schlüssel, prallen alle Anfragen ab, die nicht den passenden Schlüssel im Gepäck haben.

Bei der Anmeldung mit Schlüsseln (Public-Key-Authentifizierung) handelt es sich um ein Verfahren der asymmetrischen Kryptografie. Es braucht ein Schlüsselpaar, das aus einem privaten und einem öffentlichen Schlüssel besteht. Der öffentliche Schlüssel liegt auf dem Zielsystem, dem SSH-Server. Der private Schlüssel verbleibt auf Ihrem lokalen System, dem SSH-Client. Teilen Sie ihn niemals mit anderen. Bei der Public-Key-Authentifizierung initiiert der Client die SSH-Verbindung, der Server sendet dann eine verschlüsselte Nachricht. Der Client entschlüsselt die Nachricht mit seinem Private Key und schickt sie zurück an den Server. Der Server verifiziert die Nachricht, bei Erfolg ist der Client authentifiziert.

Passen Sie gut auf Ihre Schlüssel auf. Dazu gehört, sie bei der Generierung stets mit einer Passphrase zu versehen. Ein Schlüssel ohne Passphrase kann von Schurken schnell missbraucht werden. Wenn Sie Ihr SSH-Schlüsselpaar zusätzlich mit einem physischen Sicherheitsschlüssel, beispielsweise einem FIDO2-Stick absichern, können Sie unter bestimmten Umständen auch auf die Passphrase verzichten. Dazu später mehr.

Kein Schlüsselgeiz

Grundsätzlich sollten Sie für jedes Zielsystem und Plattformen wie GitHub oder GitLab ein eigenes Schlüsselpaar generieren. Das mindert die Gefahr, dass sie unabsichtlich einen Generalschlüssel teilen, beispielsweise weil Sie ihn durch einen Konfigurationsfehler in ein öffentliches Code-Repository laden. Auf Linux- und macOS-Systemen landen generierte Schlüsselpaare standardmäßig im Verzeichnis ~/.ssh. Erstellen Sie mit folgendem Befehl ein Schlüsselpaar:

```
ssh-keygen -t ed25519 \
-f ~/.ssh/cttest.ed25519 \
-C "Schlüssel von ndi"
```

Der Parameter `-t ed25519` gibt an, dass der Schlüssel mittels elliptischer Kurve vom Typ ed25519 erstellt werden soll. Dabei handelt es sich um ein modernes Verfahren, das schnell und sicher Schlüssel erzeugt, die viel kürzer sein dürfen als RSA-Schlüssel. Mit der Option `-f ~/.ssh/cttest.ed25519` bestimmen Sie den Dateinamen und den Speicherort. Passen Sie den Namen nach Belieben an. Mit dem Parameter `-C` versehen Sie den Schlüssel mit einem Kommentar, beispielsweise Kontaktdaten. Das ist insbesondere nützlich, um den richtigen Schlüssel mittels SSH-Agent zu identifizieren, wenn sich irgendwann viele Schlüssel in ~/.ssh tummeln. `ssh-keygen` erzeugt zwei Dateien: In der mit dem angegebenen Namen steckt der private Schlüssel, in einer weiteren mit der zusätzlichen Endung .pub der dazugehörige öffentliche.

Schlüsseltransfer

Damit Ihr Schlüssel für die sichere Anmeldung an einem entfernten System taugt, müssen Sie ihn erstmal dorthin auf die Reise schicken. Das geht am einfachsten mit dem Befehl `ssh-copy-id`:

```
ssh-copy-id -i \
~/.ssh/cttest.ed25519.pub \
ndi@example.com
```

Ersetzen Sie Pfad und Dateiname durch Ihren öffentlichen Schlüssel. Der obige Befehl geht davon aus, dass die Anmeldung via Passwort noch aktiv ist und Sie noch nicht auf dem entfernten Server angemeldet sind. Falls Sie bereits eine laufende SSH-Session haben, können Sie sich alternativ auch auf dem SSH-Client Ihren Public Key anzeigen lassen:

```
cat ~/.ssh/cttest.ed25519.pub
```

Kopieren Sie dann einfach die Ausgabe und tragen den Schlüssel auf dem Server in die Datei `authorized_keys` ein. Die befindet sich standardmäßig im Verzeichnis /home/$USERNAME/.ssh/. Achtung: In der Eile kopieren viele versehentlich den privaten Schlüssel auf den Server – der hat dort nichts verloren. Achten Sie darauf, nur die Datei mit der Endung .pub zu kopieren.

Vergewissern Sie sich, dass Sie eine SSH-Verbindung mittels Public-Key-Authentifizierung herstellen können, indem Sie die laufende SSH-Session beenden und sich mit folgendem Befehl erneut am entfernten System anmelden:

```
ssh ndi@example.com
```

Für die Anmeldung sollten Sie jetzt nur noch nach der Passphrase gefragt werden, die Sie bei der Generierung des Schlüsselpaars festgelegt haben, und nicht mehr nach Ihrem Passwort auf dem SSH-Server. Falls Sie mehrere Schlüssel in Ihrem lokalen ~/.ssh-Verzeichnis haben, dann helfen Sie OpenSSH auf die Sprünge, indem Sie den Pfad zum korrekten Schlüssel angeben:

```
ssh -i ~/.ssh/cttest.ed25519 \
ndi@example.com
```

Wenn Sie sich vergewissert haben, dass die Authentifizierung mittels Schlüssel funktioniert, dann sollten Sie die Anmeldung via Passwort deaktivieren. Überspringen Sie die Prüfung der Anmeldung nicht, Sie könnten sich aussperren! Richten Sie ein zweites Schlüsselpaar ein und bewahren Sie Ihren privaten Schlüssel an einem sicheren Ort auf, damit Sie den Server auch erreichen können, falls Ihr Hauptschlüssel mal verloren geht.

Deaktivieren Sie die Passwortanmeldung, indem Sie die Datei /etc/ssh/sshd_config auf dem Server mit einem Texteditor bearbeiten und in den Zeilen `PasswordAuthentication` und `ChallengeResponseAuthentication` das `yes` durch `no` ersetzen:

```
PasswordAuthentication no
ChallengeResponseAuthentication no
```

Starten Sie dann den SSH-Dienst neu, um die geänderte Konfiguration zu laden. Die aktive SSH-Verbindung bleibt bestehen:

```
systemctl restart ssh
```

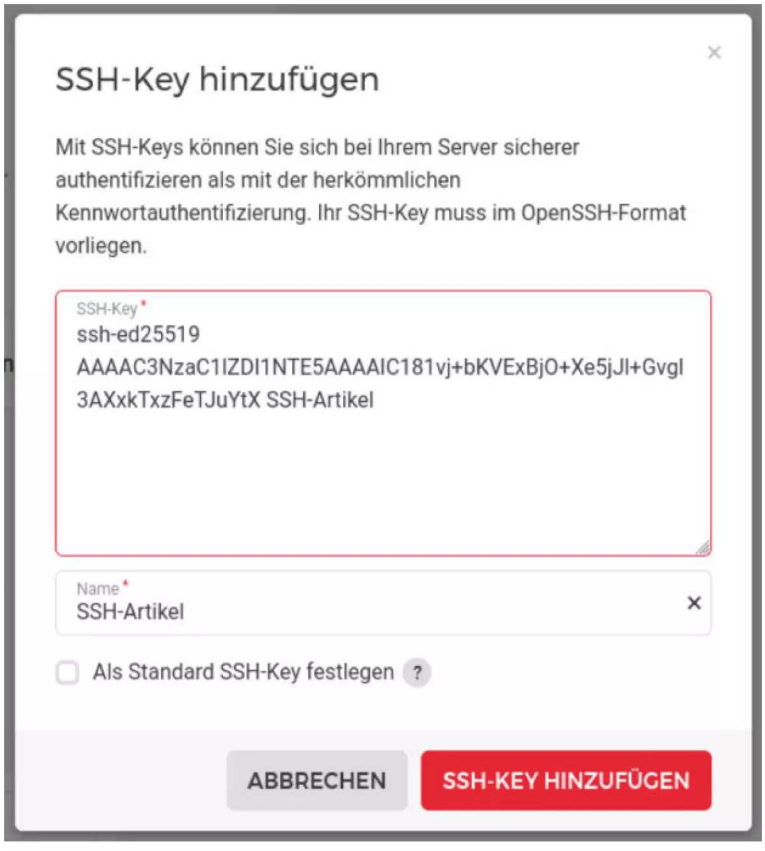
Sie müssen keine Schlüssel verschicken und das System nachträglich zusperren, wenn Sie dem Server den öffentlichen Schlüssel bereits bei der Einrichtung mit auf den Weg geben. Anbieter von Cloudservern, aber auch Hypervisor wie Proxmox nutzen zur automatischen Konfiguration ihrer VPS (Virtual Private Server) und VMs das sogenannte Cloud-Init-Verfahren. Sie können Ihren öffentlichen Schlüssel dann einfach in der Weboberfläche des Anbieters eintragen. Das funktioniert so ähnlich auch mit dem Raspberry Pi Imager, wenn Sie damit Raspberry Pi OS auf eine SD-Karte schreiben. Falls Sie Größeres vorhaben: Mit Tools für IaC (Infrastructure-as-Code) wie Terraform verfüttern Sie Ihren öffentlichen Schlüssel mit wenigen Code-Schnipseln an eine ganze Serverflotte.

Abkürzung

Das Passwort sind Sie bereits losgeworden, aber noch müssen Sie sich Benutzer- und Hostname oder IP-Adresse des Servers merken. Das können Sie sich ebenfalls sparen, indem Sie auf Ihrem Client die Datei ~/.ssh/config anlegen und Ihre Konfiguration dort hinterlegen. An dieser Stelle lohnt sich der Hinweis, dass OpenSSH seine Konfiguration in dieser Reihenfolge aus den folgenden Quellen bezieht: erst die Kommandozeilenoptionen, dann die Konfigurationsdatei des Nutzers ~/.ssh/config und schlussendlich die systemweite Konfigurationsdatei /etc/ssh/ssh_config. SSH schnappt sich jeweils den ersten vorgefundenen Wert.

Ein Beispiel für eine simple SSH-Konfigurationsdatei sieht so aus:

```
Host cttest
     HostName cttest.example.com
     User ndi
     IdentityFile␣
↳~/.ssh/cttest.ed25519
```



Cloud-Provider nutzen Cloud-Init, um VPS-Instanzen den öffentlichen Schlüssel mit auf den Weg zu geben. Ein Root-Passwort via Mail zu verschicken, wo es abgefangen werden könnte, ist dann nicht mehr nötig.

```
Host cttest2
     HostName
     cttest2.example.com
     User ndi
     Port 2222
     LocalForward 80 localhost:8080
     IdentityFile ↴
     ↳~/.ssh/cttest2.ed25519
```

Tragen Sie beim Schlüssel `Host` ein Alias für Ihren SSH-Server ein. Wählen Sie am besten einen kurzen und eingängigen Namen. Als `HostName` tragen Sie den Hostnamen oder die IP-Adresse Ihres Servers ein. Hier kann es praktisch sein, mit Wildcards (Platzhalterzeichen) zu arbeiten, beispielsweise `*.local` für alle Server in Ihrem Heimnetz. Beim Schlüssel `User` legen Sie das Benutzerkonto auf dem Server fest, mit dem Sie sich verbinden. Mit `IdentityFile` definieren Sie, welchen Schlüssel der SSH-Client bei der Public-Key-Authentifizierung vorzeigt.

Sie können beliebig viele Hosts ergänzen und die Werte Ihren Anforderungen anpassen, beispielsweise den SSH-Client anweisen, einen abweichenden Port anzusprechen, einen lokalen Port an den SSH-Server durchzureichen oder über einen SSH-Jump-Host auf einen Server in einem nicht-öffentlichen Netzwerk springen. Mit dem Befehl `man ssh_config` verschaffen Sie sich einen Überblick über die Möglichkeiten.

Nachdem Sie Ihren SSH-Client wie im Beispiel eingerichtet haben, können Sie sich mit den konfigurierten Servern einfach mit einem Befehl nach dem Muster `ssh cttest` verbinden und brauchen sich keine Hostnamen, Benutzernamen und Schlüssel mehr zu merken.

Sicherheitsschlüssel-Schlüssel

OpenSSH beherrscht seit Version 8.2 die Fähigkeit, SSH-Schlüssel an FIDO2-kompatible Sicherheitsschlüssel wie den YubiKey oder Nitrokey zu binden. Dazu braucht es öffentliche Schlüssel, die im Format ecdsa-sk oder ed25519-sk vorliegen, der Zusatz „sk“ steht für „Security Key“. Besonders praktisch: Sie können Ihren SSH-Schlüssel auch als sogenannten „Resident Key“ einrichten, auch „Discoverable Credentials“ genannt.

Vorausgesetzt, Sie haben Ihren FIDO2-Sicherheitsschlüssel stets dabei, sind Sie damit direkt an jedem beliebigen SSH-Client einsatzbereit. Damit das funktioniert, müssen Sie Ihrem FIDO2-Schlüssel eine PIN verpassen. Das erledigen Sie auf Linux-Systemen für den YubiKey mit der Software „YubiKey Manager“, die der Hersteller als AppImage zur Verfügung stellt. Alternativ greifen Sie zum Kommandozeilenwerkzeug ykman, (auch „YubiKey Manager CLI“ genannt). Eine Installationsanleitung sowie Downloads für Windows und macOS haben wir unter ct.de/wfa8 verlinkt. Laut YubiKey-Dokumentation ist SSH mit FIDO2 unter Windows noch in Arbeit. Beim Nitrokey braucht es für die PIN das Helferlein pynitrokey (siehe ct.de/wfa8). Grundsätzliches zur Zwei-Faktor-Authentifizierung und FIDO2 haben wir bereits in [1] aufgeschrieben.

Zunächst generieren Sie ein FIDO2-kompatibles Schlüsselpaar mit folgendem Befehl:

```
ssh-keygen -t ed25519-sk \
-f ~/.ssh/fido2-cttest.ed25519-sk \
-O resident -O verify-required
```

OpenSSH fragt jetzt Ihre PIN ab und fordert Sie auf, Ihren Sicherheitsschlüssel zu berühren. Sie können zur zusätzlichen Absicherung auch eine Passphrase für den Schlüssel vergeben. Für die ed25519-Kurve brauchen Sie einen YubiKey mit Firmwareversion 5.2.3 oder neuer, beispielsweise den YubiKey 5C, 5C nano oder 5 NFC. Nutzen Sie andernfalls das ecdsa-Verfahren.

Die Option `-O resident` erleichtert den Schlüssel auf anderen Clients zu nutzen. Mit `-O verify-required` müssen Sie sich stets mit Ihrer PIN ausweisen, wenn der SSH-Schlüssel zum Einsatz kommt. Das ist sicherer, denn standardmäßig verlangt OpenSSH nur die Präsenz eines Benutzers, die dieser durch Berühren des Sicherheitsschlüssels signalisiert. So könnte ein Angreifer, der Ihren FIDO2-Stick stiehlt, sich Ihres SSH-Schlüssels bedienen, falls Sie ihn nicht zusätzlich durch eine Passphrase gesichert haben. Für Resident Keys brauchen sowohl Client als auch Server OpenSSH 8.3 oder neuer.

In Ihrem ~/.ssh-Verzeichnis liegen nun zwei Dateien namens fido2-cttest.ed25519-sk und fido2-cttest.ed25519-sk.pub. Der öffentliche Schlüssel unterscheidet sich nicht von den vorigen öffentlichen Schlüsseln. Sie befördern ihn wie gewohnt durch Copy & Paste, via `ssh-copy-id` oder schon bei der Einrichtung des SSH-Servers in die Datei `authorized_keys` oder tragen ihn in GitHub oder Gitlab ein. Das, was wie der private Schlüssel aussieht, ist tatsächlich nur ein Derivat des privaten Schlüssels. Es wird mit dem Geheimnis erzeugt, das im FIDO2-Schlüssel steckt (siehe dazu ct.de/wfa8). Das Geheimnis verlässt den Schlüssel nie und kann nicht ausgelesen werden.

Melden Sie sich jetzt mit dem SSH-Schlüssel, der an den FIDO2-Stick gebunden ist, an einem SSH-Server an:

```
ssh -i ~/.ssh/fido2-cttest\
.ed25519-sk ndi@example.com
```

Alternativ tragen Sie wie zuvor beschrieben das Benutzerkonto, Hostnamen und den passenden Schlüssel in Ihre SSH-Konfigurationsdatei ein. Berühren Sie den FIDO2-Stick und authentifizieren Sie sich mit Ihrer PIN (und Ihrer Passphrase, wenn Sie eine vergeben haben).

Allzeit bereit

Mit dem Resident Key auf dem FIDO2-Stick legen Sie auf jedem System mit laufendem SSH-Agent sofort los. Stecken Sie den Sicherheitsschlüssel ein, und importieren Sie den Resident Key für die laufende Session:

```
ssh-add -K
```

Die eigenen SSH-Schlüssel mit einem FIDO2-kompatiblen Sicherheitsschlüssel zu verknüpfen, schafft eine zusätzliche Hürde für Angreifer. Je nachdem, wie Sie Ihre Schlüssel einrichten, können Sie sie auf beliebigen Clients verwenden.

Um Ihren SSH-Schlüssel freizugeben, müssen Sie den leuchtenden FIDO2-Stick berühren und sich mit Ihrer PIN authentifizieren.

Im Anschluss weisen Sie mit dem Befehl `ssh-add -L` den SSH-Agent an, die verfügbaren Schlüssel aufzulisten. Ihr FIDO2-Resident-Key sollte darunter sein.

Sie können den privaten Schlüssel jetzt auf dem neuen System nutzen, um sich mittels Public-Key-Verfahren zu authentifizieren. Er überlebt allerdings keinen Reboot. Um das Schlüsselpaar dauerhaft zu importieren, navigieren Sie in das Verzeichnis ~/.ssh und führen folgenden Befehl aus:

```
ssh-keygen -K
```

SSH legt nun beide Teile des Schlüsselpaares in das Verzeichnis. Resident Keys haben den Vorteil, dass sie mobil sind und überall genutzt werden können. Wenn Ihnen das nicht geheuer ist, dann können Sie Ihr Schlüsselpaar auch als „Non-Discoverable Credentials“ einrichten. Es ist dann erforderlich, dass der private Schlüssel sowohl im ~/.ssh-Verzeichnis des eingeloggten Benutzers als auch im FIDO2-Sicherheitsschlüssel hinterlegt ist. Um einen solchen Schlüssel zu erstellen, lassen Sie die Option `-O resident` einfach weg.

Die Dokumentation des YubiKey rät dazu, serverseitig nur Schlüssel zu erlauben, die eine Authentifizierung mittels PIN erfordern. Dazu ergänzen Sie in der Datei /etc/ssh/sshd_config folgende Zeile:

```
PubkeyAuthOptions verify-required
```

Die Option hat keine Auswirkungen auf gewöhnliche öffentliche Schlüssel, die nicht mit einem FIDO2-Sicherheitsschlüssel gekoppelt sind.

Ein YubiKey der 5er-Serie fasst bis zu 25 Resident Keys. Mit dem Befehl `ykman fido list` listen Sie die Kennungen aller hinterlegten Schlüssel auf. `ykman delete` gefolgt von der Kennung löscht den Schlüssel vom FIDO2-Stick. Sie müssen den Vorgang durch Eingabe Ihrer PIN bestätigen. Denken Sie daran, dass Verlust und Defekt bei einem FIDO2-Stick nicht ausgeschlossen werden können. Verlassen Sie sich deshalb nie auf eine einzige Möglichkeit zur Authentifizierung. Wie Sie es vermeiden, sich mit Zwei-Faktor-Authentifizierung selbst auszusperren, lesen Sie in [2].

Übernehmen Sie!

Sie kennen jetzt eine Reihe von Ansätzen, um sich den Alltag mit SSH zu erleichtern, ohne dabei Security-Kompromisse einzugehen. Verzichten Sie auf die Anmeldung mittels Passwort und setzen Sie stattdessen auf die bessere Public-Key-Authentifizierung. Hüten Sie Ihren Schlüsselbund: Schützen Sie Schlüssel mindestens mit einer Passphrase, besser mit einem FIDO2-Sicherheitsschlüssel. Mit einem Resident Key sind Sie überall sofort einsatzbereit. Tüfteln Sie an Ihrer SSH-Konfiguration und lassen Sie die config die Fleißarbeit für Sie erledigen. Haben Sie Spaß mit der Secure Shell! (ndi) c't

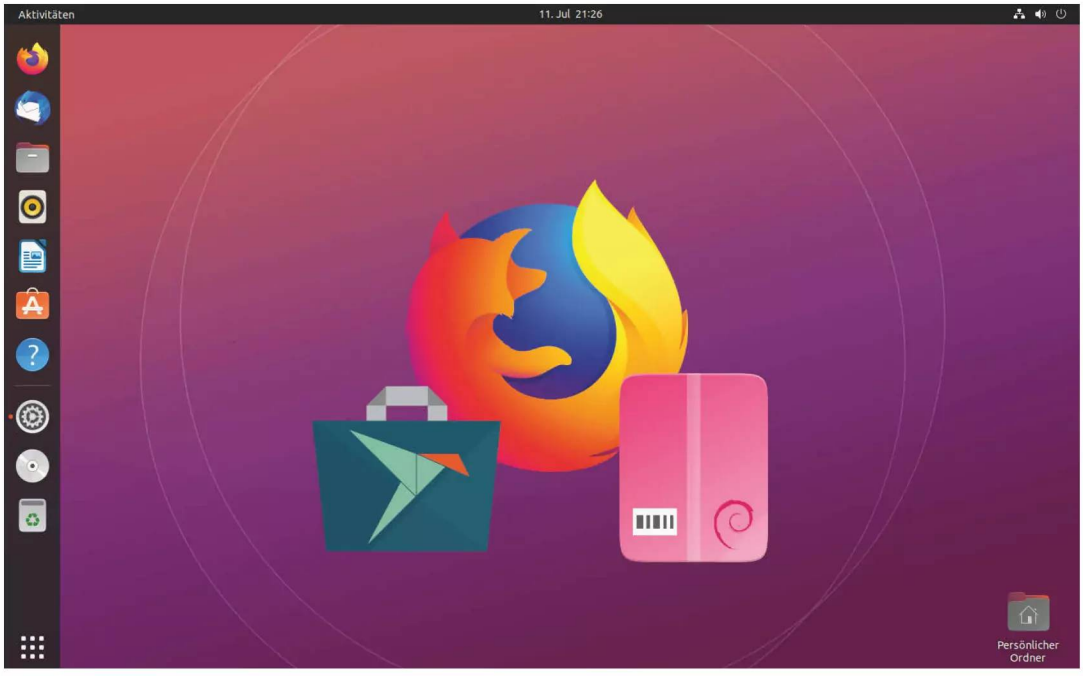
Literatur

[1] Niklas Dierking, Ronald Eikenberg, Schlosskombination, Verfahren und Geräte für sichere Online-Zugänge, c't 9/2022, S. 18

[2] Jan Mahn, Größte anzunehmende Unfälle, Zwei-Faktor-Strategie ohne Frust bei Verlust, c't 9/2022, S. 30

Dokumentation und Downloads

ct.de/wfa8



Firefox in Ubuntu: APT statt Snap

Seit der Ubuntu-Version 22.04 installiert Firefox nur aus dem Snap-Store, was einige Nachteile bringt. Mit dieser Anleitung wechseln Sie zurück zum klassisch installierten Firefox, ohne an Sicherheit einzubüßen.

Von **Keywan Tonekaboni**

Canonical hat gute Gründe dafür, Firefox standardmäßig als Snap-Paket einzurichten: Die Pflege und Aktualisierung im Snap-Store übernimmt Mozilla selbst, womit die aktuelle Firefox-Version deutlich schneller auf den Rechner gelangt. Zudem laufen Snap-Programme abgeschottet in einer Sandbox. Das soll verhindern, dass bei einer Sicherheitslücke Tür und Tor ins System offenstehen. Allerdings macht gerade die Sandbox Probleme, denn sie kappt Schnittstellen zwischen dem Browser und anderen Programmen, wie Passwortmanagern. Ubuntu-Hersteller Canonical arbeitet bereits an einer Lösung, doch bis dahin füllt zum Beispiel KeepassXC keine Passwortfelder aus.

Wenn Sie diese Probleme nicht plagen, sollten Sie beim Snap-Firefox bleiben. Die Umstellung ist seit Ubuntu 22.04 LTS nicht ganz trivial, da Canonical in diesem Release Firefox nicht mehr über die Apt-

Paketquellen ausliefert. Das vorhandene Paket ist ein Platzhalter und installiert lediglich Firefox aus dem Snap-Store.

Das DEB-Paket des Firefox-Browsers liefert das PPA (Personal Package Archive) „Firefox ESR and Thunderbird stable builds“ (siehe ct.de/wbcg). Dort stellt Ubuntus Mozilla-Team unter anderem für Ubuntu 22.04 LTS (Codename „Jammy“) aktuelle Pakete von Firefox, Firefox ESR und Thunderbird bereit.

Wir empfehlen die Installation des älteren Firefox ESR (Extended Support Release). Zwar hinkt er der normalen Firefox-Version hinterher. Allerdings nutzt er andere Dateinamen und Pfade und beugt so einem Kuddelmuddel der Firefox-Einstellungen mit den offiziellen Paketen vor. Sollten Sie Ihr Ubuntu-System von Ubuntu 20.04 LTS oder 21.10 auf die aktuelle Version aktualisiert haben, öffnen Sie ein Terminal und entfernen mit `sudo apt remove firefox` das überflüssige Übergangspaket.

Firefox-PPA fixieren

Bevor Sie das PPA hinzufügen, bereiten Sie Apt auf die Fremdpakete vor. Die Paketverwaltung soll künftig Firefox ESR aus dem PPA bevorzugen, andere Pakete wie Thunderbird aus diesem Repository jedoch ignorieren. Das regeln Sie über Apt-Pinning. Legen Sie dazu mit Root-Rechten im Verzeichnis /etc/apt/preferences.d/ die Datei mozillateam mit folgendem Inhalt an:

```
Package: *
Pin: release o=LP-PPA-mozillateam
Pin-Priority: 100

Package: firefox-esr*
Pin: release o=LP-PPA-mozillateam
Pin-Priority: 600
```

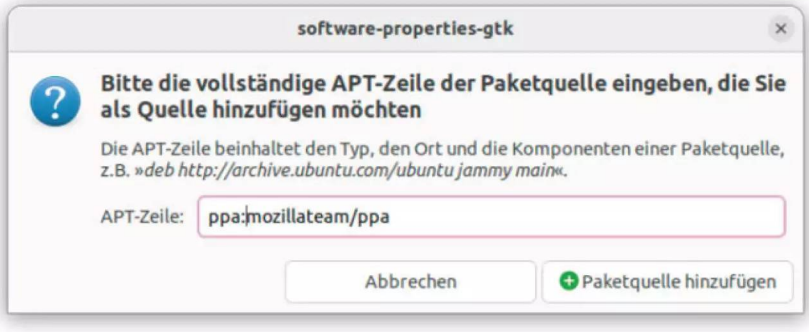
Die Konfiguration weist allen Paketen (Package: *) des Herausgebers „LP-PPA-mozillateam“ eine geringe Priorität zu. Beim Wert 100 installiert Apt Pakete aus dieser Quelle nie automatisch. Der zweite Block erhöht für alle Pakete, deren Name mit „firefox-esr“ beginnt, die Priorität auf 600. Da das über dem Standardwert von 500 liegt, gibt Apt Paketen aus dieser Quelle bei Updates den Vorzug.

Fügen Sie nun das PPA als Paketquelle hinzu, indem Sie „Anwendungen & Aktualisierungen“ öffnen und zum Reiter „Andere Programme“ wechseln. Klicken Sie auf „Hinzufügen …“ und geben dann hinter „APT-Zeile“ `ppa:mozillateam/ppa` ein. Nachdem Sie auf „Paketquelle hinzufügen“ geklickt haben, wandelt Ubuntu das PPA-Kürzel in eine korrekte Apt-Zeile um und importiert den öffentlichen PGP-Schlüssel des PPA. Diesen benötigt Apt, um die kryptografische Signatur der heruntergeladenen Pakete zu überprüfen, bevor es sie installiert. Schließen Sie „Anwendungen & Aktualisierungen“ und bestätigen Sie das Neuladen der Paketquellen.

Alternativ öffnen Sie ein Terminal und geben folgende Befehle ein, die ebenfalls das PPA hinzufügen und die Paketquellen aktualisieren.

```
sudo add-apt-repository ppa:mozillateam/ppa
sudo apt update
```

Sobald die aktualisiert ist, kontrollieren Sie im Terminal mit `apt policy firefox thunderbird` das Pinning. Als Installationskandidat sollte die Version von archive.ubuntu.com gekennzeichnet sein und vor der URL ppa.launchpadcontent.net der Wert 100 stehen. Die Ausgabe des Befehls `apt policy firefox-esr` sollte in der Versionstabelle hinter der Versionsnummer den Wert 600 ausspucken. Falls nicht, kontrollieren



Damit Ubuntu Firefox aus einem Personal Package Archive installiert, muss man es in „Anwendungen & Aktualisierung" als Paketquelle eintragen.

Sie im Verzeichnis /etc/apt/preferences.d/ die Angaben.

Installieren Sie nun Firefox ESR mit folgendem Befehl:

```
sudo apt install --no-install-recommends ↴
                ↳firefox-esr firefox-esr-locale-de
```

Das Kommando rüstet gleichzeitig auch die deutsche Übersetzung nach, lässt aber andere, unnötige Zusatzpakete außen vor.

Starten Sie nach Abschluss der Installation den Browser mit dem Befehl `firefox-esr`. Wichtig: Die Eingabe von `firefox` öffnet noch die Snap-Version.

Verknüpfungen verbiegen

Damit nicht aus Versehen die Snap-Variante startet, legen Sie zunächst im Terminal eine neue Verknüpfung an, die den Befehl `firefox` auf Firefox ESR umbiegt.

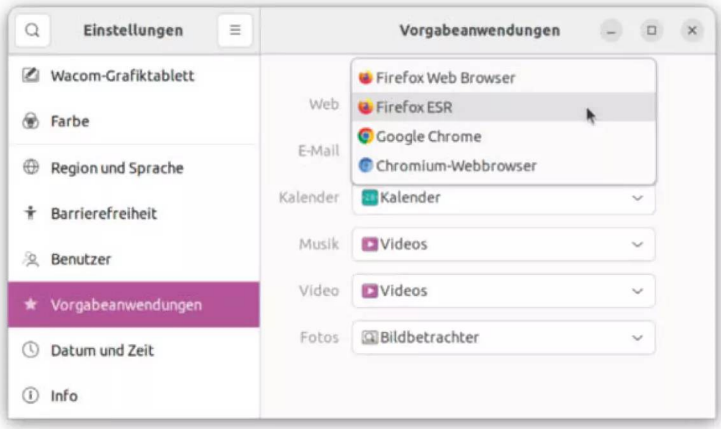
```
sudo ln -s /usr/bin/firefox-esr ↴
         ↳/usr/local/bin/firefox
```

Wenn Sie in der Bedienoberfläche nach Firefox suchen, tauchen nun meist zwei identische Einträge auf – ohne einen Hinweis, welche Version sich hinter welchem Icon verbirgt. Um die Einträge anzupassen, kopieren Sie zunächst die Datei firefox-esr.desktop aus dem Verzeichnis /usr/share/applications/ nach ~/.local/share/applications. Öffnen Sie diese Kopie dann in einem Texteditor und ändern Sie die Zeile „Name=…“ zu „Name=Firefox ESR“. Wenige Sekunden nach dem Speichern der Datei sollte der neue Name in der Anwendungssuche auftauchen. Ändern Sie danach in den Systemeinstellungen unter „Vorgabeanwendungen/Web“ den Browser auf Firefox ESR.

Sollte der Eintrag in der Auswahlliste fehlen, erzwingen Sie den Wechsel über folgenden Befehl (ohne Root/sudo):

```
xdg-settings set default-web-browser ↴
                ↳firefox-esr.desktop
```

Soll der Desktop die Snap-Variante im Desktop komplett ausblenden, kopieren Sie auch die Datei /var/lib/snapd/desktop/applications/firefox_firefox.desktop nach ~/.local/share/applications. Fügen Sie in dieser Datei unterhalb von `[Desktop Entry]` die Anweisung `NoDisplay=true` in einer eigenen Zeile hinzu.



Um nicht versehentlich den falschen Browser zu starten, machen Sie Firefox ESR zur Vorgabeanwendung fürs Web.

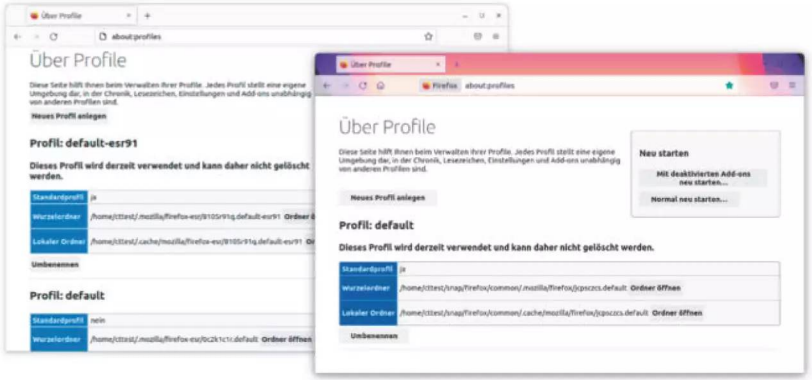
Die Snap-Version von Firefox können Sie weiterhin über den Befehle `snap run firefox` starten.

Firefox ESR speichert seine Einstellungen in einem anderen Verzeichnis als die zuvor aktive Variante, daher startet der Browser mit einem frischen Profil. Das muss nicht schlecht sein, denn so schleppen Sie keinen alten Ballast mit. Wenn Sie ihr vorheriges Firefox-Profil nicht importieren wollen, können Sie bereits fröhlich lossurfen. Falls Ihr Firefox-Profil erhaltenswerte Daten enthält – beispielsweise gespeicherte Zugangsdaten, Lesezeichen oder Chronik-Einträge – steht Ihnen noch ein Arbeitsschritt bevor.

Profil portieren

Ein bequemer Weg, Ihr Profil zu importieren, ist der Onlinedienst Firefox Sync, für den Sie bei Mozilla ein Konto anlegen müssen. Die Funktion finden Sie ganz oben im Hauptmenü unter „Daten synchronisieren und speichern“. Was synchronisiert wird, legen Sie unter „Einstellungen/Synchronisation“ fest. Richten Sie Firefox Sync zuerst im alten Browser (Firefox Snap) ein, danach im neuen.

Ohne den Onlinedienst müssen Sie den Umzug eigenständig stemmen. Wollen Sie nur Ihre Lesezeichen mitnehmen, reicht es, diese im alten Browser aus der Bibliothek zu exportieren. Das ist einfacher und weniger fehleranfällig, als das gesamte Profil mitzunehmen. Öffnen Sie dazu im vorherigen Firefox die Lesezeichen-Verwaltung (Bibliothek) mit Strg+Umschalt+O und speichern Sie über „Importieren und Sichern/Sichern …“ Ihre Lesezeichen als JSON-Datei. Wechseln Sie dann zum neu installierten Firefox und importieren Sie



Auf der Spezialseite „about:profiles“ verrät Firefox den Pfad zum jeweiligen Profil.

Konfigurationsdateien
ct.de/wbcg

dort die JSON-Datei über „Importieren .../Wiederherstellen/Datei wählen ...“.

Soll doch das ganze Profil umziehen, öffnen Sie die Seite „about:profiles“ in beiden Browser-Varianten und klicken jeweils beim verwendeten Profil in der Zeile „Wurzelordner“ auf die Schaltfläche „Ordner öffnen“, um die Profil-Verzeichnisse im Dateimanager zu öffnen. Schließen Sie dann alle Browser-Fenster und beenden Sie beide Firefox-Varianten. Kopieren Sie nun mit dem Dateimanager den Inhalt des Snap-Profils (in der Regel „~/snap/firefox/common/.mozilla/firefox/...default“) ins neue ESR-Profil (üblicherweise „~/.mozilla/firefox-esr/...default-esr91“). Überschreiben Sie alle vorhandenen Dateien im Zielverzeichnis. Damit Firefox ESR das neuere Profil akzeptiert, öffnen Sie ihn diesmal über ein Terminalfenster mit:

```
firefox-esr --allow-downgrade -P
```

Wählen Sie im Profil-Manager anschließend das gewünschte Profil aus, meist „default-release“ oder schlicht „default“.

Zu guter Letzt ist es praktisch, in beiden Firefox-Varianten unterschiedliche Themes einzustellen (außer Sie nutzen Firefox Sync). So sehen Sie auf einen Blick, welchen Firefox Sie vor sich haben. (ktn) ct

Backup-Programme für den Linux-Desktop

Um unter Linux seine Daten regelmäßig und komfortabel zu sichern, gibt es gleich eine ganze Palette quelloffener Backup-Programme. Doch nicht alle begeistern in unserem Test.

Von **Tim Schürmann**

Bild: Andreas Martini

Zwei Stunden vor dem wichtigen Termin lässt sich plötzlich die Präsentation nicht mehr öffnen. Wohl dem, der dann ein Backup besitzt. Um sich gegen Datenträgerdefekte, Schusseligkeit, Brände und andere Katastrophen zu wappnen, sind nicht nur im Homeoffice regelmäßige Sicherungen Pflicht. Unterstützung bei dieser lästigen Aufgabe offerieren unter Linux zahlreiche Open-Source-Werkzeuge. Diese Backup-Tools setzt man einmal auf die zu sichernden Daten an und kann sich dann bequem zurücklehnen – zumindest im Idealfall. Mit solchen Programmen haben selbst Backup-Muffel oder weniger technikaffine Nutzer keine Ausrede mehr für fehlende Sicherungen.

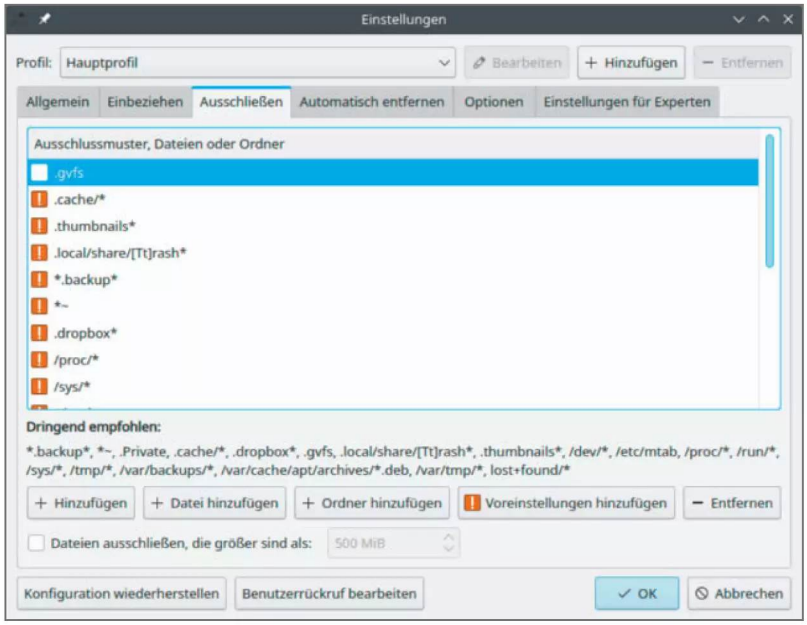
Backup leichtgemacht

Wir haben fünf Backup-Anwendungen mit grafischer Bedienoberfläche auf den Prüfstand geholt, die eine möglichst einfache Bedienung versprechen und sich auf die Sicherung der Nutzerdaten konzentrieren: Back In Time, Déjà Dup, Duplicati, Kup und Vorta. Außen vor bleiben Kommandozeilenwerkzeuge wie BorgBackup oder Duplicity, bei deren Inbetriebnahme man mit kryptischen Parametern jonglieren muss. Einfach zu bedienende grafische Frontends für solche Terminal-Programme haben wir aber ins Testfeld aufgenommen. Die Backup-Programme müssen die Kriterien erfüllen, die für robuste Datensicherungen minimal notwendig sind: automatische Backups nach Zeitplan, Sicherung auf einem externen Datenträger und Wiederherstellung mit allen Dateiattributen.

Besser das Backup liegt auf einem externen Datenträger, dann reißt ein defektes Notebook nicht auch noch die Sicherung mit ins Verderben. Orientieren kann man sich dabei an der 3-2-1-Regel: Man erstellt drei Kopien auf mindestens zwei verschiedenen Datenträgern, von denen einer außer Haus lagert. Für Letzteres bietet sich ein Cloudspeicherdienst an. Bastler können alternativ Tools wie syncosync nutzen [1]. Damit bei einer Sicherung die anfallenden Datenmengen möglichst klein bleiben, sollten die Backup-Tools nur die geänderten Daten sichern (inkrementelles Backup). Des Weiteren sollte die Wiederherstellung möglichst einfach gelingen und auch die Dateiattribute, wie etwa das Erstellungsdatum, rekonstruieren. Unsere fünf Testkandidaten versprechen all diese grundlegenden Funktionen.

Pika Backup bleibt beim Test außen vor, da es zeitgesteuerte Sicherungen erst unterstützte, als wir unsere Testläufe bereits abgeschlossen hatten. Wir stellen das Tool aber separat im Artikel „Pica-bello“ auf Seite 103 vor. Außen vor bleiben auch das auf unseren Systemen nur instabil laufende Qt-fsarchiver sowie KBackup, dem eine Funktion zur Wiederherstellung fehlt. Ebenfalls durchs Raster fielen Backup-Lösungen für Unternehmen, die eine komplexe Konfiguration erfordern und meist nach dem Client-Server-Prinzip funktionieren. Auch Tools, die komplette Datenträger sichern, haben wir nicht berücksichtigt. Hierzu zählen beispielsweise Rescuezilla und Clonezilla. Diese Werkzeuge kommen in der Regel in Form eines Live-Systems und sind daher für eine tägliche Sicherung weniger praktikabel. Sie eignen sich allerdings hervorragend, um hin und wieder das komplette Betriebssystem zu sichern. Wer im Internet nach Backup-Programmen für Linux fahndet, stolpert zudem über veraltete Werkzeuge und eingeschlafene Projekte, wie etwa Flyback, KDar, Simple Backup und das in Linux Mint enthaltene mintBackup. Diesen Tools sollte man seine Daten sicherheitshalber nicht anvertrauen.

Die meisten Programme lassen sich unkompliziert über die Softwareverwaltung der Distributionen installieren. Nur bei Duplicati muss man selbst



Back In Time schlägt zahlreiche Dateien und Verzeichnisse vor, die es beim Backup auslassen will. Darunter sind vor allem Caches und temporäre Dateien.

ein DEB- oder RPM-Paket von der Projekt-Website herunterladen und einspielen. Das gelingt jedoch meist per Doppelklick auf das Paket, um Abhängigkeiten kümmert sich die Paketverwaltung.

Sicherungsziele

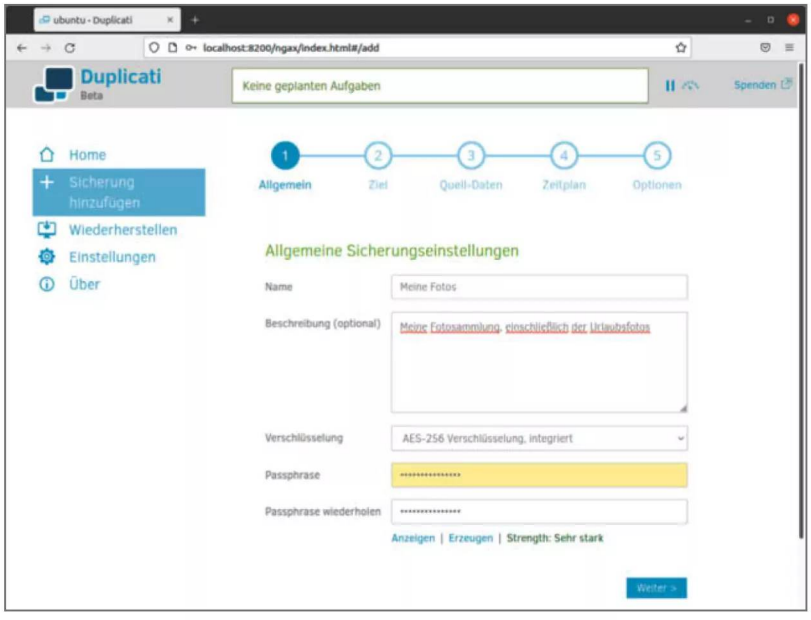
Sämtliche Backup-Programme legen ihre Sicherungen in einem beliebigen Verzeichnis ab. Soll das Backup auf einen externen Datenträger wandern, muss man diesen zuvor in ein Verzeichnis mounten lassen. Solange Linux das Dateisystem erkennt, legen alle Programme ihre Sicherungen darauf ab. Back In Time und Kup können auf das Anstöpseln des Backup-Laufwerks warten und dann umgehend darauf sichern. Kup lauert sogar auf das Einhängen eines Verzeichnisses. Déjà Dup holt zeitgesteuerte Backups nach, sobald das Ziel-Laufwerk verfügbar ist. Duplicati und Vorta können direkt vor und nach einem Backup ein beliebiges Shell-Skript aufrufen, das dann beispielsweise eine Datenbank herunterfährt oder Daten aus einer Anwendung exportiert.

SMB-Freigaben, etwa von einem NAS, muss man vor dem Backup manuell mounten. Nur Déjà Dup bindet Freigaben direkt ein, aber den Pfad dorthin muss man händisch eintippen. Wer einen Dateiserver mit SSH betreibt, überträgt die Daten sicher per SFTP oder SSH, was alle bis auf Kup verstehen. Bei Vorta muss für SSH auf dem Zielrechner BorgBackup installiert sein. Vom unsicheren und veralteten FTP sollte man Abstand nehmen, weshalb wir es im Test nicht berücksichtigt haben. Ebenfalls ausgeklammert haben wir WebDAV. Das Protokoll erweist sich unseren Erfahrungen nach immer wieder als instabil.

Clouddienste wie Dropbox stehen bei den meisten Tools nicht hoch im Kurs. Duplicati hingegen spricht mit rund 20 Diensten, darunter Dropbox, Google Drive und Microsoft OneDrive. Déjà Dup beliefert immerhin Google Drive und Microsoft OneDrive direkt, Vorta bietet nur das von dessen Autor betriebene und recht unbekannte BorgBase.com an, aber man kann auch andere BorgBackup-Hoster wie rsync.net oder Hetzner nutzen. In jedem Fall kann man als Behelfslösung das Backup in einem lokalen Verzeichnis ablegen und dieses dann vom Client des Cloudanbieters mit der Wolke synchronisieren lassen.

Ein- und Ausschluss

Die zu sichernden Verzeichnisse und Dateien hakt man bei Duplicati und Kup bequem in einem Dateibaum ab. Bei Back In Time, Déjà Dup und Vorta muss man sie umständlich nacheinander mit einem Dialogfenster auswählen. Sämtliche Backup-Tools laufen mit den Rechten ihres Benutzers. Folglich können sie nur solche Dateien verarbeiten, auf die auch der Benutzer zugreifen darf. Für die Sicherung von Systemdateien oder kompletter Systeme sind die Programme nicht ausgelegt, selbst wenn man sie per `sudo` startet. Nur Back In Time fordert erweiterte Rechte per Polkit an, sofern man es über `backintime_qt-polkit` startet.



Duplicati führt den Anwender schrittweise zu einem neuen Backup und schätzt bei einer Verschlüsselung sogar die Qualität des Passworts ein.

Über eine Ausschlussliste lassen sich bei allen Tools gezielt einzelne Dateien und Verzeichnisse von der Sicherung ausnehmen. Teilweise gelingt das bequem per Mausklick, sonst muss man die Dateinamen der zu ignorierenden Störenfriede eintragen, wobei Platzhalter wie „*.bak“ oder sogar reguläre Ausdrücke erlaubt sind. In Duplicati klickt man Ausschlusskriterien per Maus zusammen.

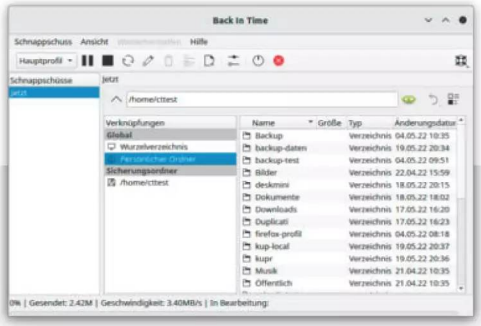
Darüber hinaus können Back In Time und Duplicati gezielt alle Dateien ausschließen, die eine wählbare Größe überschreiten. Sämtliche Backup-Tools sichern auch versteckte Dateien. Vorsicht: Bei der Auswahl der zu sichernden Daten zeigen die Programme standardmäßig keine versteckten Dateien

Kostenlose Backup-Software für den Linux-Desktop

Name	Back In Time	Déjà Dup	Duplicati	Kup	Vorta
Hersteller, URL	Back-In-Time-Team, github.com/bit-team	Gnome-Team, wiki.gnome.org/Apps/DejaDup	Duplicati-Team, duplicati.com	Kup-Team,invent.kde.org/system/kup	Vorta-Team, vorta.borgbase.com
Version / Lizenz	1.3.3 / GPLv2	44.2 / GPLv3	2.0.7.1 / LGPLv2.1	0.9.1 / GPLv2	0.8.12 / GPLv3
Anwendungsdetails					
erhältlich für Arch / Debian / Ubuntu / Fedora / openSUSE	✓ / ✓ / ✓ (PPA) / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓	✓ (AUR) / ✓[2] / ✓[2] / ✓[2] / ✓[2]	✓ / ✓ / ✓ / – / ✓	✓ / ✓ / ✓ / ✓ / ✓
verfügbar via Flathub / Snap	– / –	✓ / ✓	– / –	– / –	✓ / –
Frontend für	Rsync	Duplicity	–	Bup (Rsync[5])	BorgBackup
Desktop-Integration	–	Gnome	Panel-Applet	KDE Plasma	Panel-Applet
Sicherung auf					
lokaler Datenträger / Unix-Dateisystem notwendig	✓ / – (aber Hardlinks)	✓ / –	✓ / –	✓ / – (✓[5])	✓ / –
SSH / SFTP / SMB	✓ / – / –	✓ / ✓ / ✓	✓ / ✓ / –	– / – / –	✓[6] / – / –
Clouddienst	–	Google Drive, OneDrive	Dropbox, Google Drive, OneDrive, Amazon S3 und weitere	–	BorgBase.com, BorgBackup-Hoster (z.B. rsync.net, Hetzner)
Upload-Drosselung	✓	–	✓	–	–
Ablageformat	einzelne Dateien	Archiv	Archiv	Archiv (einzelne Dateien[5])	Archiv (Repository)
Verschlüsselung / Kompression	✓ / –	✓ / ✓	✓ / ✓	– / ✓ (–[5])	✓ / ✓
Sicherungsfunktionen					
Dateien / Ordner	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
Einschlusslisten	Hinzufügen	Hinzufügen	Liste, Filter, Regex	Liste	Hinzufügen
Ausschlusslisten	Manuelle Eingabe, Muster	Hinzufügen	Hinzufügen, Filter, Regex	Regex	Muster
Intervalle frei wählbar	beliebig	täglich, wöchentlich	beliebig	beliebig, aktive Nutzung	beliebig
Autostart bei Mount	✓	✓ (bei Zeitsteuerung)	–	✓	–
Protokolle / Fehlermeldung	✓ / ✓ (Benachrichtigung)	– / ✓ (Benachrichtigung)	✓ / ✓ (Benachrichtigung, E-Mail)	✓ / ✓ (Benachrichtigung)	✓ / ✓ (Benachrichtigung)
Integrität prüfen automatisch / manuell	– / –	– / –	✓ / ✓	✓ / –	✓ / ✓
inkrementelle / differentielle	✓ / –	✓ / –	✓ / ✓	✓ (–[5]) /	–[7] / –
deduplizierend	–	–	✓	✓	✓
Backup-Archive aufsplitten	–	✓ (automatisch)	✓	–	–
Vollbackups: Intervall / manuell starten	frei wählbar / ✓	frei wählbar (Tage, Wochen) / ✓	frei wählbar / ✓	frei wählbar / ✓	frei wählbar / ✓
alte Backups löschen: automatisch / manuell	✓ / ✓	✓ / –	✓ / –	– / ✓	✓ / ✓
Wiederherstellung					
fehlerhaftes Backup erkennen / wiederherstellen	– / –	– / –[3]	✓ / ✓	✓ / ✓	✓ / ✓
einzelne Dateien / bestimmte Versionen wiederherstellen	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
Backups durchsuchbar	–	✓	✓	–	–
Attribute: Zugriffsrechte / Gruppe / Symbolische Links / Hardlinks	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓[4]	✓ / – / ✓ / ✓	✓ / – / ✓ / ✓
Funktionstests					
Sicherungsdauer[1] (NVMe-SSD / USB3-HDD)	1:57 min / 8:01 min	18:48 min / 20:51 min	14:27 min / 14:35 min	11:59 min / 16:55 min	3:43 min / 6:35 min
Speicherplatz[1]: Erstsicherung / Inkrementell	27 GByte / 2 GByte	26 GByte / 1 GByte	26 GByte / 2 GByte	24 GByte / 2 GByte	25 GByte / 1 GByte
Bewertung					
Zuverlässigkeit	○	○	⊕⊕	⊕	⊕
Funktionsumfang	⊕	○	⊕⊕	⊕	⊕⊕
Bedienkomfort	⊕	⊕⊕	⊕	⊕	○
Geschwindigkeit	⊕	○	○	○	⊕⊕

[1] Testordner: 27 GByte + 1,5 GByte inkrementelle Daten [2] RPM oder DEB als Download [3] Wiederherstellung bis zum fehlerhaften Datensatz [4] nicht mit Standardeinstellungen [5] im Synchronisations-Modus
[6] BorgBackup muss auf Zielsystem installiert sein [7] blockweise Deduplizierung über gesamtes Backup-Repository

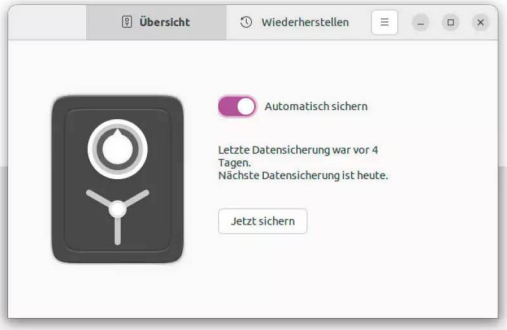
✓ vorhanden – nicht vorhanden ⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht



Back In Time

Back In Time sichert die ausgewählten Dateien mit dem Kommandozeilenprogramm Rsync. Jedes neu angestoßene Backup landet Datei für Datei in einem eigenen Unterverzeichnis. Für unveränderte Dateien legt Back In Time Hardlinks an. Das spart Speicherplatz, schließt aber viele SMB-Server oder NAS als Sicherungsziel aus, da sie keine Hardlinks verstehen. Das inkrementelle Backup auf der externen Festplatte dauerte sehr lang. Geänderte Dateien erkennt Back In Time am Änderungsdatum oder mittels Prüfsummen. Die Einstellungen sind verteilt auf übersichtliche Registerkarten. Das Hauptfenster zeigt die Inhalte einer Sicherung, per Mausklick springt man schnell zu einer älteren Fassung. Auf Wunsch vergleicht das Backup-Tool zwei Dateiversionen mit einem Diff-Programm. Back In Time kann im Akkubetrieb die Sicherungen aussetzen. Auf Wunsch schaltet das Tool nach einer Sicherung automatisch den Rechner aus.

- **einfache Bedienung**
- **intelligentes Löschen alter Backups**
- **erstellt keine Archive**



Déjà Dup

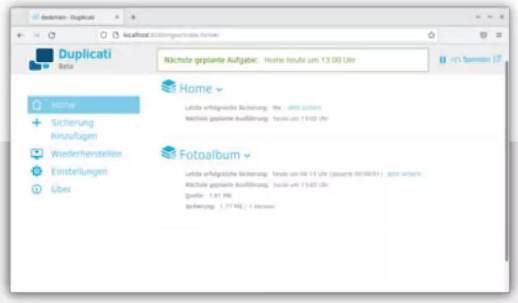
Déjà Dup stellt das Backup-Programm des Gnome-Desktops. Für seine Arbeiten spannt es im Hintergrund das Backup-Tool Duplicity ein, die automatische Sicherung stößt der Hintergrunddienst „deja-dup-monitor“ an. Viele Distributionen mit Gnome-Desktop installieren Déjà Dup standardmäßig. In der Regel macht es sich kurze Zeit nach dem Start mit einer Aufforderung zur Datensicherung bemerkbar. Ein Assistent führt mit wenigen Mausklicks selbst Computerlaien zu ihrem ersten Backup: Man klickt sich die zu sichernden Verzeichnisse zusammen, wählt den Speicherort und knipst gegebenenfalls die Verschlüsselung an. Der Zugriff auf die gesicherten Dateien erfolgt im Hauptfenster, dessen Aufbau dem eines kargen Gnome-Dateimanagers ähnelt. Wie bei den meisten Gnome-Anwendungen ist diese Schlichtheit von den Entwicklern gewollt, auch wenn Duplicity deutlich mehr Funktionen bietet.

- **sehr einfache Bedienung**
- **gute Integration in Gnome**
- **rudimentärer Funktionsumfang**

an, sichern sie aber kommentarlos mit. So kann beispielsweise „~/.cache“ unbemerkt das Backup um mehrere unnütze GByte aufblähen.

Paketdienste

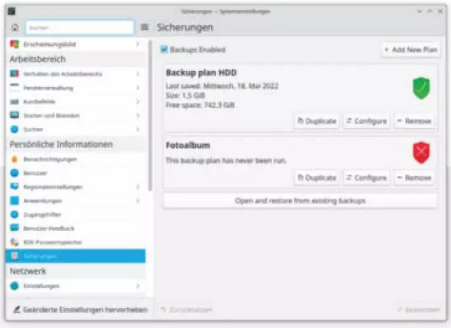
Fast alle Tools packen die zu sichernden Dateien in ein Archiv. Dabei erhalten sie die Dateiattribute, wie etwa das Erstellungsdatum. Die Backup-Archive von Déjà Dup, Duplicati und Kup verwenden ein eigenes Format. Sie lassen sich folglich später nur mit dem entsprechenden Backup-Tool wiederherstellen. Vorta speichert mit BorgBackup die Dateien im Repository, dessen Arbeitsweise wir im Artikel „Daten sichern mit BorgBackup“ auf Seite 108 erklären. Duplicati verteilt das Backup bei Bedarf auf mehrere Archive,



Duplicati

Duplicati startet als Hintergrunddienst, der eine aufgeräumte Weboberfläche bereitstellt. Diese versteckt allerdings Feineinstellungen, etwa zum Kompressionsverfahren, in den fummelig zu bedienenden „Optionen für Profis“. Der Zugang zur Weboberfläche lässt sich mit einem Passwort sichern. Backups kann man auch von einem anderen Rechner aus anstoßen. Bei Problemen meldet sich Duplicati per E-Mail. Duplicati setzt das .NET-Framework Mono voraus. Die Installation vereinfachen fertige DEB- und RPM-Pakete. Arch-Linux-Nutzer finden Duplicati im AUR. Die aktuelle Version „2.0 (beta)“ arbeitet stabil. Anders als unter Windows, kann das Tool unter Linux nicht direkt auf SMB-Freigaben zugreifen. Die muss man vorher selbst einhängen. Standardmäßig verschickt Duplicati Nutzungsdaten an seine Entwickler.

- **übersichtliche Bedienoberfläche**
- **unterstützt viele Clouddienste**
- **erweiterte Optionen umständlich**

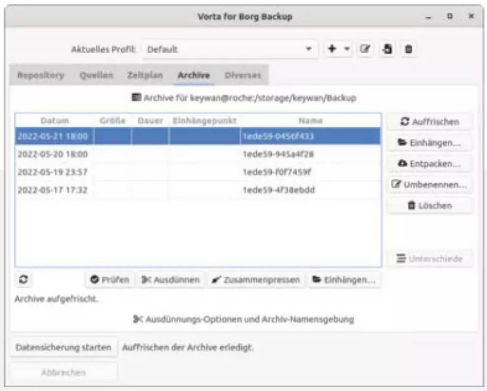


Kup

Kup lässt sich nur mit KDE Plasma sinnvoll nutzen. Die Konfiguration erfolgt in der Systemsteuerung des Plasma-Desktops. Das Backup-Tool steuert man über ein Applet in der Kontrollleiste, was in der Praxis umständlich ist. Die eigentliche Sicherung übernimmt das Backupprogramm Bup. Alle Dateien landen in einem Archiv mit inkrementellen Backups. Kup kennt einen zweiten Sicherungsmodus mit Rsync: Hier synchronisiert es lediglich den aktuellen Stand aller Dateien mit einem Backup-Verzeichnis. Dabei bleiben die Dateiattribute nur auf Unix-Dateisystemen erhalten. Auf Netzwerkfreigaben speichert Kup nur, wenn die vorher eingehängt sind. Kup bringt ein Modul für das KIO-Framework mit, worüber man aus allen KDE-Anwendungen direkt auf die Inhalte des Archivs zugreifen können soll – auf unserem Testsystem wollte das jedoch nicht gelingen.

- **gute Integration in KDE Plasma**
- **funktioniert nur mit KDE Plasma**
- **umständliche Applet-Bedienung**

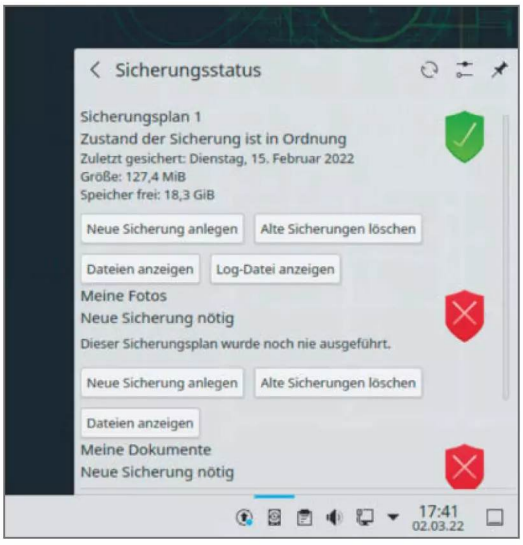
deren maximale Größe sich frei wählen lässt. Hilfreich ist diese Aufteilung vor allem bei Clouddiensten und auf Servern mit einem Größenlimit. Beim Up- und Download von Backups können Duplicati und Back In Time die Geschwindigkeiten drosseln, um zum Beispiel den Internetzugang nicht mit einer laufenden Sicherung zu verstopfen; Vorta nur indirekt über einen Kommandozeilenparameter für Borg-Backup. Back In Time sichert alle Dateien einzeln in ein Backup-Verzeichnis und merkt sich wichtige Metadaten in einer separaten Datei. Damit lassen sich die Backups auf Dateisystemen ablegen, die keine Unix-Dateiattribute unterstützten. Allerdings sollte man dort tunlichst nicht das Backup-Verzeichnis verändern, um das Tool nicht aus dem Tritt zu bringen.



Vorta

Vorta basiert auf dem Backup-Tool BorgBackup. Dessen Einstellungen offeriert Vorta auf mehreren überladenen Registern mit jeweils weiteren Unterregistern. Einsteiger könnten sich davon überfordert fühlen. Umgekehrt dürfen BorgBackup-Experten beliebige weitere Parameter an das Tool durchreichen. Den Ablageort für die Backups muss man erst initialisieren, wobei Vorta im Zielverzeichnis passende Unterverzeichnisse anlegt. Die Verbindung zu einem Ablageort kann man jederzeit (vorübergehend) lösen, beispielsweise wenn man im Hotel keinen Zugriff auf den Onlinespeicher hat. Bei der Verschlüsselung spannt Vorta die Passwortverwaltung der Desktopumgebung ein. Sofern „llfuse“ installiert ist, lässt sich eine Sicherung wie ein Datenträger schreibgeschützt mounten. Auf Wunsch sichert Vorta nur über vorgegebene Netzwerke.

- **viele Optionen und Funktionen**
- **verschlüsselte Verbindungen**
- **Kenntnisse in BorgBackup nötig**



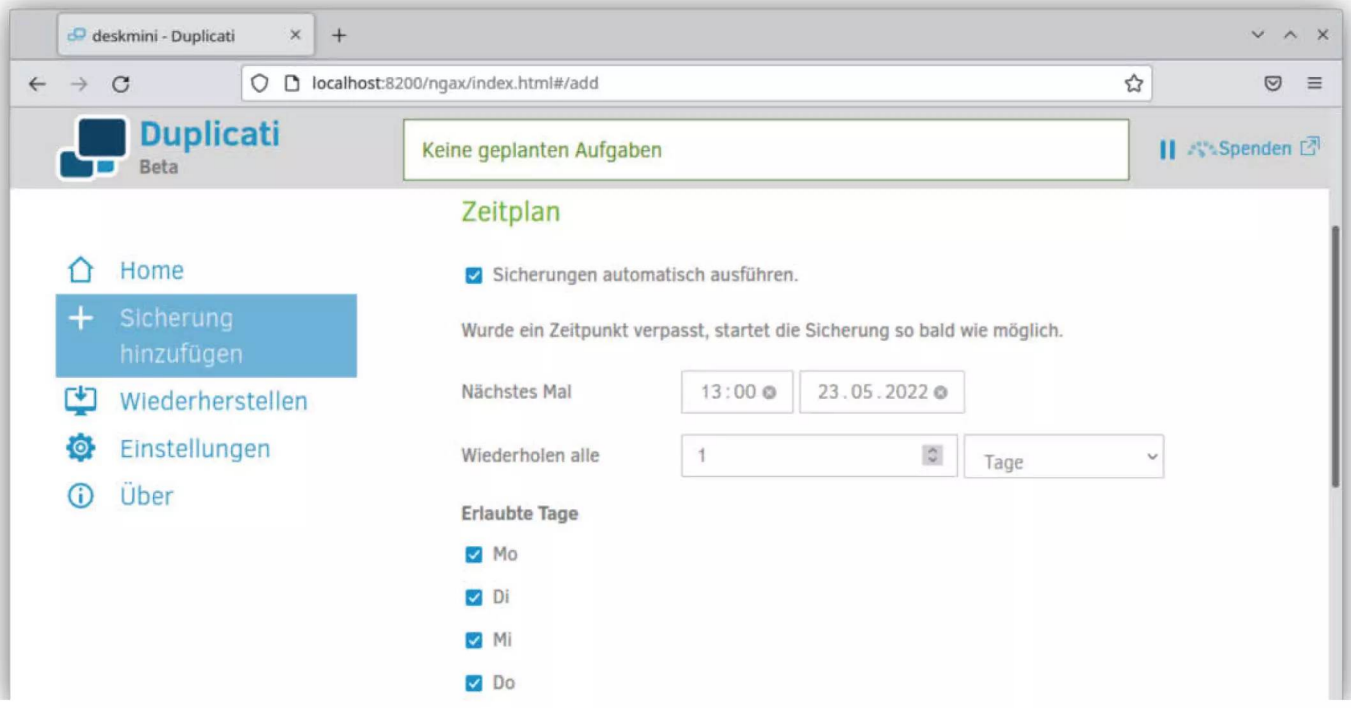
Kup steuert man ausschließlich über das Applet in der Kontrollleiste.

Damit das Backup möglichst wenig Platz belegt und bei einem Upload in die Cloud nur wenig Bandbreite schluckt, komprimieren bis auf Back In Time alle Tools die Sicherung. Duplicati und Vorta gehen sogar noch einen Schritt weiter und speichern identische Datenblöcke nur einmal. Nicht nur zwei identische Fotos belegen bei dieser sogenannten Deduplizierung im Backup nur den Platz eines Exemplars, sondern auch bei Dateien mit ähnlichen Inhalten speichern die Tools Platz ein.

Um weiteren Speicherplatz zu sparen, sichern sämtliche Testkandidaten nur die Dateien, die sich seit dem letzten Backup verändert haben. Bei der Wiederherstellung benötigt man allerdings zwingend das erste vollständige Backup und alle darauf aufbauenden Teilsicherungen. Vorta hat alle Versionen im Repository und stellt den benötigten Datensatz effizient daraus wieder her. Ein beschädigtes Teilbackup oder Repository kann die komplette Sicherung unbrauchbar machen. Keines der sechs Tools unterstützt die etwas größeren, aber robusteren differentiellen Backups. Auch deshalb ist das 3-2-1-Prinzip so wichtig. Déjà Dup geht immerhin einen Mittelweg, indem es in regelmäßigen Abständen ein vollständiges Backup erstellt. Kup kann zudem seine Archive mit zusätzlichen Informationen anreichern, die später bei einem Defekt der Sicherung die Wahrscheinlichkeit einer Wiederherstellung erhöhen.

Wecker

Die Backup-Programme erstellen die Sicherungen in regelmäßigen Abständen automatisch. Die Intervalle darf man selbst festlegen, wobei die Möglichkeiten zwischen den Tools weit auseinander gehen.



Duplicati führt ein Backup otional nur an vorgegebenen Wochentagen durch.

So kann etwa Déjà Dup nur täglich oder wöchentlich Sicherungen erstellen, während Back In Time, Duplicati und Vorta sogar im Minutentakt sichern könnten. Kup sichert die Daten auf Wunsch auch automatisch nach ein paar Stunden aktiver Arbeit am Computer.

Sollte der Rechner zum eigentlichen Backup-Termin ausgeschaltet sein, holen Duplicati, Kup und Vorta die Sicherung zum nächstmöglichen Zeitpunkt nach – vorausgesetzt, man hat die entsprechende Einstellung aktiviert. Bei Verbindungsabbrüchen zum Server oder Clouddienst setzt Duplicati die Sicherung später fort.

Persönliche Daten sollten nur verschlüsselt im Backup landen. Das gilt insbesondere bei der Nutzung eines Clouddienstes. Eine Verschlüsselung bieten nur Déjà Dup, Duplicati und Vorta an, wobei bei Letzterem die Auswahl des Verschlüsselungsmodus aufgrund kryptischer Bezeichnungen wie „repokey-blake2“ unnötig schwer fällt.

Backup-Hilfen

Bis auf Déjà Dup nehmen alle Backup-Programme unterschiedliche Sicherungsaufträge entgegen – beispielsweise einen für die gelegentliche Sicherung der Fotosammlung und einen zweiten, häufigeren für die übrigen Dokumente.

Alle Tools melden fehlgeschlagene Backups direkt in der Bedienoberfläche oder als Systemnachricht. Back In Time, Duplicati und Kup liefern auf Knopfdruck ein ausführliches Protokoll, Vorta nur eines, das mit Informationen geizt. Statt eine verständliche Fehlermeldung auszuspucken, lassen Déjà Dup, Kup und Vorta manchmal die User mit einem Traceback allein, mit dem nur Programmierer etwas anfangen können.

Ein defektes Backup wäre der GAU. Bessere Programme untersuchen daher die Sicherungen möglichst regelmäßig auf ihre Unversehrtheit. Während Back In Time und Déjà Dup überhaupt nicht die Integrität prüfen, nehmen Duplicati, Kup und Vorta das Backup regelmäßig unter die Lupe. Bei Kup muss man diese wichtige Maßnahme erst einschalten, zudem prüft das Tool das Backup-Archiv nur vor jedem neuen (inkrementellen) Sicherungsvorgang. Duplicati wiederum lädt regelmäßig Teile des Backups aus der Cloud und versucht, sie wiederherzustellen. Sollte die Sicherung in der Cloud defekt sein, repariert sie Duplicati mit den auf der Festplatte vorhandenen Daten. Nur

bei Duplicati und Vorta kann man die Prüfung auch manuell anstoßen.

Wiederherstellung

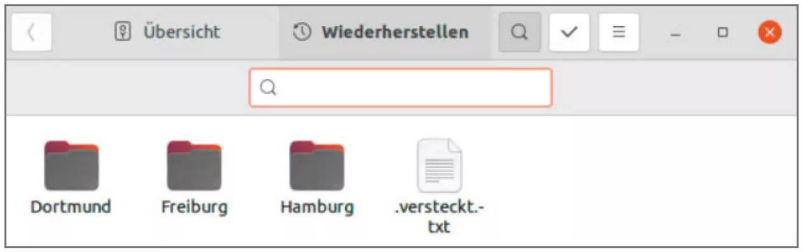
In Déjà Dup, Duplicati, Kup und Vorta darf man einzelne Dateien aus der Sicherung herausfischen, Déjà Dup und Duplicati bieten sogar eine Suchfunktion. Vorta kann das Backup schreibgeschützt in ein Verzeichnis einhängen, wo es sich mit einem Dateibrowser durchstöbern lässt. Back In Time sichert die Dateien einzeln, dort kann man direkt auf die gesicherten Dateien zugreifen. Ergänzend bietet Back In Time eine Wiederherstellungsfunktion an, die alle Dateiattribute erhält. Sofern die Backup-Programme unter einem normalen Nutzerkonto laufen, gehören nach der Wiederherstellung sämtliche Dateien dem aktuellen Benutzer.

Damit der Platz auf dem Backup-Medium nicht irgendwann ausgeht, löschen alle Tools bis auf Kup automatisch ältere Sicherungen. Bei den zugehörigen Einstellungen sind Back In Time, Duplicati und Vorta besonders flexibel.

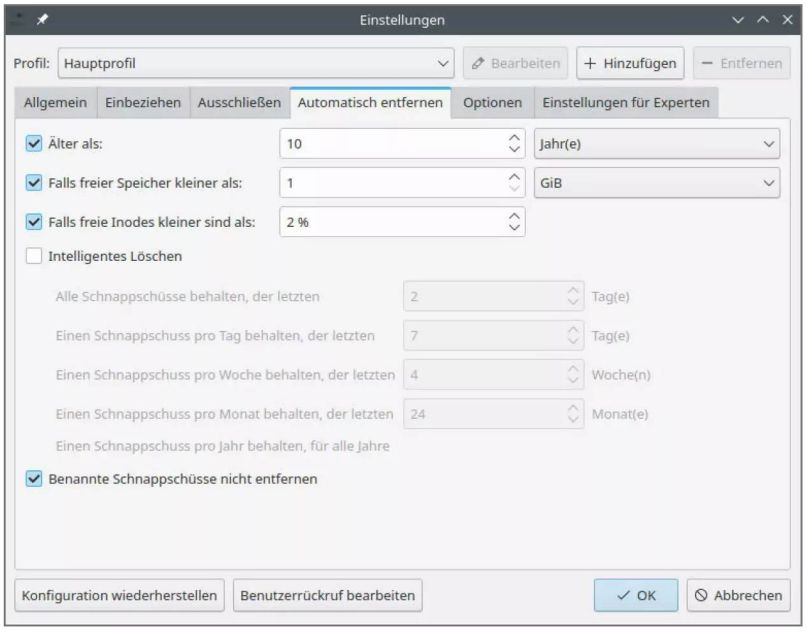
Die Sicherung des kompletten Systems stellt die Backup-Programme vor besondere Herausforderungen: Zum einen müssen die Dateirechte erhalten bleiben und zum anderen sind ständig einige Dateien geöffnet und somit für einen weiteren Zugriff blockiert. Am ehesten gelang das Duplicati und Vorta, aber keines der Programme in unserem Test war für ein Systembackup geeignet. Dafür sollte man besser auf Rescuezilla und ähnliche Tools zurückgreifen. Wie man diese Werkzeuge mit einem der hier getesteten Programme kombiniert, erklärt der nachfolgende Artikel „Backup-Strategien für Linux-Desktops“ ab Seite 104.

Fazit

Keines der getesteten Backup-Programme überzeugt in allen Disziplinen. Back In Time und Déjà Dup sichern unkompliziert die persönlichen Daten aus dem Home-Verzeichnis, aber ihnen fehlt die wichtige Integritätsprüfung. Vorta bietet einen großen Funktionsumfang an, der sich aber in der überladenen Oberfläche widerspiegelt. Den Spagat zwischen einfach und vielseitig könnten Duplicati und Kup schaffen. Leider legt Kup die Sicherungen nur unverschlüsselt ab. Duplicati spricht mit zahlreichen Clouddiensten und begeistert mit seiner einfachen Bedienung, solange man nicht eine der Profi-Optionen benötigt.



Déjà Dup zeigt die gesicherten Daten wie ein Dateimanager an. Ältere Versionen wählt man über das Datum der Sicherung.



Die Einstellungen zum Löschverhalten alter Backups sind nicht immer direkt zu durchschauen.

Sehr gut integriert in den Desktop sind Kup bei KDE Plasma und Déjà Dup in Gnome. Beide eignen sich trotz der genannten Kritikpunkte gut für Einsteiger und alle, die ohne viel Nachdenken regelmäßig ihre Daten sichern wollen. Das gilt auch für Duplicati. Für Fortgeschrittene oder unerschrockene Nutzer bietet sich Vorta an. Auch wenn nicht im Test, vereint das im folgenden Artikel „Pika-bello“ vorgestellte Pika viele der Stärken von Vorta, ist einfach zu bedienen und lässt sich gut in Gnome integrieren. Für welches Programm Sie sich auch immer entscheiden: Jedes Backup ist besser als keines. (ktn) c't

Literatur

[1] Peter Siering, Backup-Buddy, c't 13/2022, S. 88

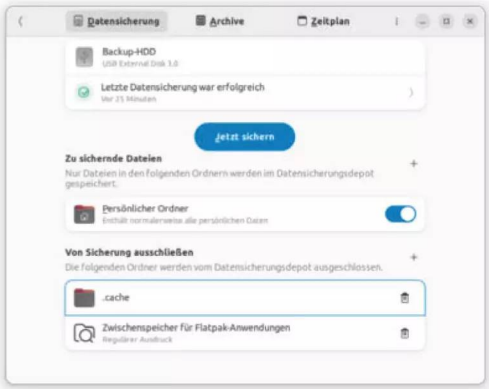
Pika-bello

Backups anlegen; schnell, sicher, zuverlässig und vor allem einfach – das verspricht das Linux-Programm Pika Datensicherung. Es dient als grafische Oberfläche für das bewährte Kommandozeilentool BorgBackup.

Von **Keywan Tonekaboni**

In der Linux-Community gilt BorgBackup als angesagt, da es die zu sichernden Daten besonders effizient speichert. Statt Datensicherungen über einen Haufen Archivdateien zu verteilen, arbeitet BorgBackup mit einem Repository, grob vergleichbar mit Git. Wer ohne Kommandozeile die Vorzüge von BorgBackup nutzen wollte, musste bisher auf Vorta zurückgreifen (siehe Kasten „Vorta“ auf S. 105). Allerdings ist Vortas Bedienoberfläche alles andere als eingängig.

Hier kommt Pika ins Spiel. Als Anwendung aus dem Gnome-Umfeld besticht das Programm mit dem typischen, sehr schlichten Design. Backup-Ziel auswählen, Passwort zum Verschlüsseln eingeben und ein Klick auf „Jetzt sichern“ – mehr braucht Pika nicht, um das persönliche Home-Verzeichnis zu sichern. Weitere Ordner fügt man einzeln per Dateiauswahldialog hinzu. In der Voreinstellung überspringt Pika den Cache-Ordner im Home-Verzeichnis. Um weitere Daten von der Sicherung auszuschließn, kann man Dateien und Verzeichnisse hinzufügen, Muster und reguläre Ausdrücke angeben oder Vorlagen verwenden, etwa um Abbilder von virtuellen Maschinen oder im Home-Verzeichnis installierte Flatpak-Anwendungen außen vor zu lassen.



Pika kann mehrere Repositories („Sicherheitsdepot“) verwalten. Es bindet vorhandene Repositories ein oder legt sie neu an; beides sowohl lokal, als auch im Netzwerk per SSH. Den Netzwerkpfad zu einem entfernten Repository muss man händisch eingeben, aber zumindest erklären Hilfstexte die Syntax der URL verständlich. Eingehängte Datenträger erkennt Pika und schlägt sie als Repository-Speicherort vor, aber auch ungeeignete Netzlaufwerke wie WebDAV-Verzeichnisse.

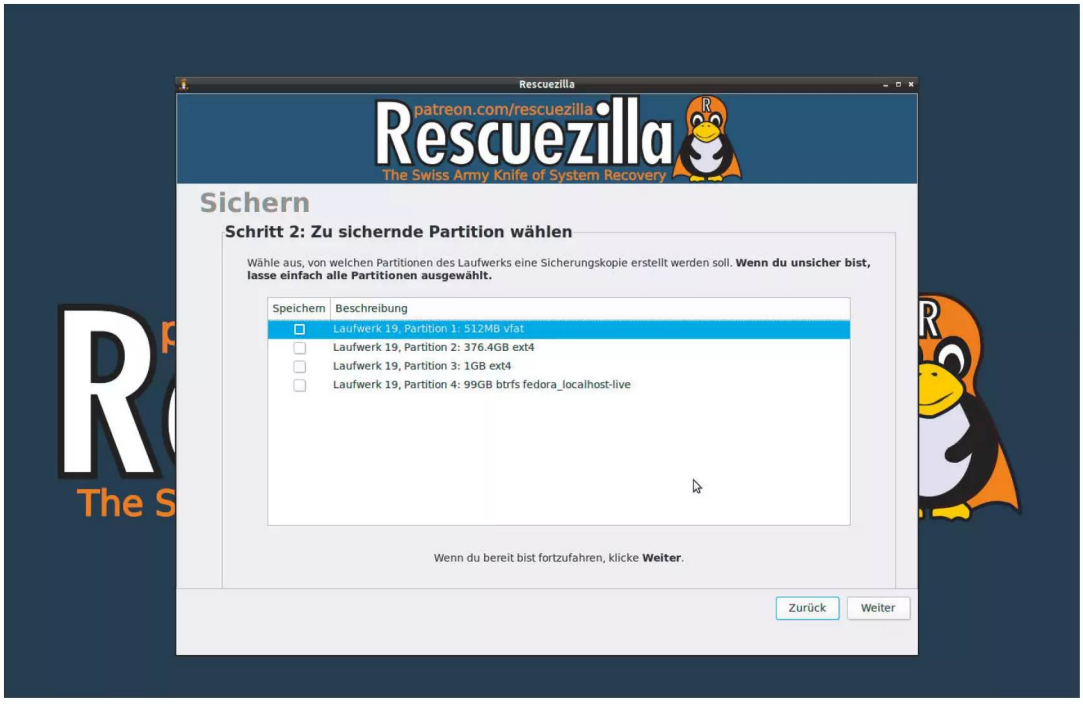
Pika Datensicherung 0.6.1

Desktop-Backup-Software	
Entwicklerin, URL	Sophie Herold, apps.gnome.org
Systemanforderungen	Linux mit Flatpak
Preis	kostenlos (GPLv3)

Auf Wunsch legt Pika neue Sicherungspunkte („Archive“) automatisch an, wahlweise stündlich, täglich, wöchentlich oder monatlich und individuell für jedes Repository. Ist zur geplanten Zeit das Backup-Ziel nicht erreichbar, holt Pika das bei nächster Gelegenheit nach, etwa sobald man die externe USB-Festplatte anschließt. Damit der Umfang des Repository nicht ausufert, kann Pika einzelne Archive gezielt entfernen („ausdünnen“), sowohl automatisch als auch manuell.

Die bereits angelegten Schnappschüsse listet Pika nach Datum sortiert auf. Möchte man eine ältere Fassung durchsuchen, hängt Pika dieses Archiv schreibgeschützt unterhalb von „~/.mnt/borg“ ein und lädt den Pfad im Dateimanager. Von dort öffnet man Dateien wie gewohnt oder kopiert Sie woanders hin. Diese Handarbeit ersetzt eine automatische Wiederherstellungsfunktion. Eine globale Suche über alle Archive bleibt Pika schuldig.

In Pikas reduzierter Programmoberfläche fehlen zwangsläufig manche Funktionen und Einstellungen. Im direkten Vergleich mit Vorta haben wir hauptsächlich die Integritätsprüfung des Repository vermisst. Das Wichtigste beim Backup ist aber, dass man es macht. Pikas Oberfläche ist angenehm einfach und allein das senkt die Hürde. (ktn) c't



Backup-Strategien für Linux-Desktops

Die Backup-Programme für Linux lassen sich zwar bequem bedienen, eignen sich aber nicht für ein komplettes Systembackup. Wir zeigen, wie Sie dennoch Ihren Linux-Desktop sichern, um im Ernstfall schnell wieder einsatzbereit zu sein.

Von **Keywan Tonekaboni**

Der Software-Test im Artikel „Backup-Programme für den Linux-Desktop“ auf Seite 94 hat gezeigt: Die Backup-Programme für den Linux-Desktop legen meist zuverlässig und bequem ein Backup des Home-Verzeichnisses des Nutzers an. Geht es darum, das komplette System zu sichern, machen sie sich aber einen schlanken Fuß. Auf manche Systemverzeichnisse können die Tools wegen eingeschränkter Rechte nicht zugreifen. Andere Daten sichern die Backup-Programme zwar, aber bei der Wiederherstellung gehen Benutzer- und Gruppenrechte verloren. Und auch wenn es naheliegend scheint: Eine grafische Anwendung mit sudo oder als Root zu starten, ist meist keine gute Idee. Neben Sicherheitsrisiken kommt noch die andere Benutzerumgebung – die von Root – hinzu, wo der Zugriff auf die gewohnte Konfiguration fehlt.

Ein Backup des Gesamtsystems aus der Desktopumgebung heraus birgt noch weitere Stolpersteine. Im laufenden Betrieb ändern sich ständig Daten, temporäre Dateien werden gelöscht und neue kommen hinzu; angeschlossene Geräte und Systemschnittstellen sind als virtuelle Dateien präsent. Das alles kann ein ackerndes Backup-Programm aus dem Tritt bringen oder endlos beschäftigen.

Aufgabenteilung

Glücklicherweise gibt es für den Job bessere Programme: Datenträger-Imager wie Rescuezilla sichern dann

Rettungsechse

Das Live-System Rescuezilla sichert komplette Partitionen mit nur wenigen Mausklicks oder klont ein vorhandenes System direkt auf einen neuen Datenträger. Obendrauf gibt es ein paar nützliche Rettungswerkzeuge.

Nach einem Hardwaredefekt, einem Virenbefall oder ähnlichen Pannen muss man häufig das gesamte System neu aufsetzen. Zeit spart dabei ein Backup des kompletten Datenträgers, das man in solchen Fällen nur in einem Stück zurückspielen muss. Genau hier greift das Live-System Rescuezilla unter die Arme: Es sichert einzelne Partitionen oder ganze Datenträger in einer großen Image-Datei und stellt sie im Fall der Fälle wieder her. Eine inkrementelle Sicherung ist dabei nicht möglich. Darüber hinaus klont Rescuezilla auf Wunsch Datenträger und Partitionen ohne den Zwischenschritt einer Sicherung auf eine neue Platte, was insbesondere bei einem Umzug auf einen neuen Computer hilft.

Anders als das Vorbild Clonezilla bietet Rescuezilla eine einfach aufgebaute grafische Bedienoberfläche. In ihr wählt man die gewünschte Funktion, sowie den Quell- und Zieldatenträger – mehr ist nicht notwendig.

Als Datenlager für die Sicherungen können neben externen Festplatten auch Netzwerklaufwerke dienen. Rescuezilla sichert den Datenträger partitionsweise und erstellt somit Backups von beliebigen Betriebssystemen. Unbenutzte Bereiche auf der Quellpartition belegen auch im Backup keinen Speicherplatz. Darüber hinaus verarbeitet das Werkzeug die Sicherungen von Clonezilla, sowie die Images der Virtualisierungslösungen VirtualBox, VMware und Qemu. Umgekehrt lassen sich Rescuezilla-Backups mit Clonezilla wiederherstellen. Aus Sicherungen kann Rescuezilla einzelne Dateien herauskopieren. Diese Funktion befindet sich noch im Beta-Stadium, insbesondere das Öffnen von komprimierten Sicherungen schlägt entweder fehl oder dauert sehr lange.

Mit an Bord sind verschiedene Rettungswerkzeuge. So reanimieren TestDisk und PhotoRec gelöschte Dokumente und Partitionen, wobei ihre Bedienung etwas Einarbeitungszeit erfordert. Weitere Tools wie der Partitionierer GParted, der Browser Firefox oder ein Dateimanager helfen beim Rettungseinsatz.

Der PC muss vom Rescuezilla-Medium, einem USB-Stick oder einer DVD booten. Dafür arbeitet es selbst dann, wenn das installierte Betriebssystem nicht mehr startet. Mit dem darunterliegenden Linux-System kommen Anwender nur bei den Datenträgerbezeichnungen in Berührung. Zwar lässt sich beim Start auch die Sprache auf Deutsch umstellen, aber einige Tools und Dialoge sprechen dann weiterhin Englisch.

Unter dem Strich erleichtert Rescuezilla es gerade weniger technikaffinen Anwendern, Komplettbackups anzulegen und wiederherzustellen. (Tim Schürmann/ktn@ct.de)

Hersteller, URL	Rescuezilla-Projekt, rescuezilla.com
Systemanf.	64-Bit-x86-System, 1 GByte RAM
Preis	**kostenlos** (GPLv3)

den gesamten Datenträger als Laufwerksabbild, samt Partitionstabelle und Bootmanager. Laden Sie von der Rescuezilla-Webseite das ISO-Image herunter (siehe ct.de/w6g5) und schreiben Sie es mit einem Programm wie Gnome Laufwerke oder balenaEtcher auf einen USB-Stick. Booten Sie von diesem Medium Ihren Computer, woraufhin Rescuezilla als Live-System startet. Folgen Sie dann einfach den Anweisungen und sichern Sie den gesamten Datenträger. Die Oberfläche ist selbsterklärend. Als Ziel für das Laufwerksabbild können Sie ein externes Medium oder ein Netzlaufwerk angeben, zum Beispiel auf einem NAS. Gibt Ihr Computer den Geist auf, starten Sie wieder das Live-System und stellen das Abbild in einem Rutsch wieder her – notfalls auch auf einem anderen als Ersatz organisierten Datenträger, wenn der über genug Platz verfügt.

Natürlich macht es mehr Mühe, das Live-System zu starten und die Sicherung anzustoßen, als wenn ein Backup-Programm die lästige Aufgabe automatisch im Hintergrund erledigt. Es reicht aber, zusätzlich zu den regelmäßigen Backups Ihres Home-Verzeichnisses hin und wieder über das Live-System ein Komplettbackup zu erzeugen, etwa nachdem Sie eine Neuinstallation fertig eingerichtet haben oder vor und nach einem Upgrade auf die neuste Version der Distribution. Wer Linux nur als Desktop-System verwendet, hat meist alle persönlichen Dateien in seinem Home-Verzeichnis beisammen.

Rettungsmanöver

Im Ernstfall stellen Sie zuerst das Abbild wieder her. Nachdem Ihr System wieder startet, aktualisieren Sie mit dem Desktop-Backup-Programm noch Ihre persönlichen Daten.

Was dann noch fehlt, sind die Apps, die Sie seit dem letzten Komplettbackup installiert haben. Doch zumindest eine Liste der Anwendungen können Sie vor der Havarie per Kommandozeile erstellen. Folgende Befehle zeigen für APT (Debian, Ubuntu & Co.), Flatpak und Snap die installierten Programme an:

```
apt list --manual-installed
flatpak list --app
snap list
```

Der apt-Aufruf listet sogar nur die von Ihnen selbst installierten Pakete auf. Packen Sie die für Sie notwendigen Befehle in ein Skript und erzeugen Sie damit innerhalb Ihres Home-Verzeichnisses eine Datei mit der Liste Ihrer installierten Anwendungen.

Für komplette Sicherungen eines Linux-Desktop-PCs sind Datenträger-Imager mit Live-System wie Rescuezilla gut geeignet.

Ein Beispielskript finden Sie unter ct.de/w6g5, was die Daten für Flatpak, Snap und aus den Paketverwaltungen von Debian/Ubuntu, Fedora und Arch abfragt. Das Skript lassen Sie regelmäßig von Cron aufrufen oder starten es vor jedem Backup. Duplicati und Vorta übernehmen das für Sie. Nach Wiederherstellung des Datenträgerabbildes und Einspielen der Home-Sicherung füttern Sie den Paketmanager mit der Liste, um die fehlenden Anwendungen und Pakete nachzuinstallieren.

Katastrophe als Chance

Sie können eine Havarie aber auch als befreienden Neustart begreifen. Mit der Zeit sammeln sich auf Computersystemen mitunter viele Altlasten. Wenn Sie der einzige User auf Ihrem Computer sind und nur schnöde Desktopanwendungen wie Firefox, LibreOffice und Gimp verwenden, warum nicht einfach das Linux-System neu installieren? Bei Ubuntu oder Fedora ist eine Neuinstallation vermutlich schneller, als Rescuezilla für eine komplette Wiederherstellung zu bemühen. Anschließend nur noch persönliche Daten und Programme einspielen und schon haben Sie ein frisches und dennoch vertrautes System zur Hand. (ktn) c't

Beispielskript und Rescuezilla-Download
ct.de/w6g5

IMPRESSUM

Redaktion

Postfach 61 04 07, 30604 Hannover
Karl-Wiechert-Allee 10, 30625 Hannover
Telefon: 05 11/53 52-300
Telefax: 05 11/53 52-417
Internet: www.heise.de

Leserbriefe und Fragen zum Heft:
sonderhefte@ct.de

Die E-Mail-Adressen der Redakteure haben die Form xx@ct.de oder xxx@ct.de. Setzen Sie statt „xx“ oder „xxx“ bitte das Redakteurs-Kürzel ein. Die Kürzel finden Sie am Ende der Artikel und hier im Impressum.

Chefredakteur: Torsten Beeck (tbe)
(verantwortlich für den Textteil)

Konzeption: Niklas Dierking (ndi)

Koordination: Jobst Kehrhahn (Leitung, keh), Pia Ehrhardt (piae), Angela Meyer (anm)

Redaktion: Niklas Dierking (ndi), Mirko Dölle (mid), Liane M. Dubowy (lmd), Pina Merkert (pmk), Angela Meyer (anm), Keywan Tonekaboni (ktn), Axel Vahldiek (axv))

Mitarbeiter dieser Ausgabe: Tim Schürmann, Alexander von Westernhagen, Rüdiger Willenberg

Assistenz: Susanne Cölle (suc), Tim Rittmeier (tir), Christopher Tränkmann (cht), Martin Triadan (mat)

DTP-Produktion: Andreas Zickert

Digitale Produktion: Christine Kreye (Ltg.), Kevin Harte, Thomas Kaltschmidt, Martin Kreft, Pascal Wissner

Fotografie: Andreas Wodrich, Melissa Ramson

Illustration: Rudolf A. Blaha, Frankfurt am Main; Andreas Martini, Wettin; Sven Hauth, Schülp; Albert Hulm, Berlin

Titel: Andreas Zickert, Midjourney

Verlag

Heise Medien GmbH & Co. KG
Postfach 61 04 07, 30604 Hannover
Karl-Wiechert-Allee 10, 30625 Hannover
Telefon: 05 11/53 52-0
Telefax: 05 11/53 52-129
Internet: www.heise.de

Herausgeber: Christian Heise, Ansgar Heise, Christian Persson

Geschäftsführer: Ansgar Heise, Beate Gerold

Mitglieder der Geschäftsleitung: Jörg Mühle, Falko Ossmann

Anzeigenleitung: Michael Hanke (-167)
(verantwortlich für den Anzeigenteil),
www.heise.de/mediadaten/ct

Anzeigenverkauf: Verlagsbüro ID GmbH & Co. KG,
Tel.: 05 11/61 65 95-0, www.verlagsbuero-id.de

Leiter Vertrieb und Marketing: André Lux (-299)

Service Sonderdrucke: Julia Conrades (-156)

Druck: Firmengruppe APPL Druck GmbH & Co. KG,
Senefelder Str. 3–11, 86650 Wemding

Vertrieb Einzelverkauf:
DMV DER MEDIENVERTRIEB GmbH & Co. KG
Meßberg 1
20086 Hamburg
Tel.: 040/3019 1800, Fax: 040/3019 145 1815
E-Mail: info@dermedienvertrieb.de
Internet: dermedienvertrieb.de

Einzelpreis: € 14,90; Schweiz CHF 27.90;
Österreich € 16,40; Luxemburg € 17,10

Erstverkaufstag: 01.08.2023

Hergestellt und produziert mit Xpublisher: www.xpublisher.com

Printed in Germany.

Bild: Erstellt mit Midjourney | Bearbeitung c't

Daten sichern mit BorgBackup

Das kostenlose und quelloffene BorgBackup nutzt eine clevere Methode für platzschonende und schnelle Datensicherungen. Wir zeigen, wie Sie mit dem Kommandozeilen-Tool für Linux- und Unix-Systeme Backups anlegen, verwalten und wiederherstellen.

Von **Tim Schürmann**

Backups nerven. Sie anzulegen ist lästig, da sie ewig dauern und die Sicherungen belegen viel Speicherplatz oder sind unhandlich auf voneinander abhängige Archivdateien verteilt. Und im Worst Case scheitert das Wiederherstellen, weil eine dieser Archivdateien beschädigt ist. Das Open-Source-Tool BorgBackup will einem diesen Kummer ersparen.

BorgBackup erzeugt nicht nur extrem platzsparende und verschlüsselte Backups, sondern prüft auch ihre Integrität. Auf Wunsch schiebt es die Sicherungen über eine SSH-Verbindung auf einen Server. Die Backups lassen sich zudem wie ein Datenträger einhängen und dann bequem mit dem favorisierten Dateimanager durchstöbern. Da man BorgBackup über den Befehl `borg` startet, wird das Backup-Tool meist nur Borg genannt. Als Kommandozeilenprogramm prädestiniert sich Borg für Server und in Shell-Skripten. Mit Vorta und Pika (siehe Artikel „Backup-Programme für den Linux-Desktop“ auf Seite 94 und „Pika-bello“ auf Seite 103) existieren auch zwei auf dem Tool aufbauende grafische Bedienoberflächen für den Linux-Desktop.

In diesem Praxisartikel zeigen wir Ihnen, wie Borg arbeitet und wie Sie über die Kommandozeile Backups anlegen, prüfen und wiederherstellen sowie über Skripte steuern. Selbst wenn Sie die Programme mit grafischer Bedienoberfläche bevorzugen, hilft Ihnen das Wissen, verlässliche Backups für den Ernstfall zu erzeugen und auch ohne laufende Desktopumgebung an Ihre Daten zu kommen.

Arbeitsweise

Borg sammelt alle zu sichernden Dateien in einem Repository. Diese Lagerstätte ist ein Verzeichnis mit einer besonderen Dateistruktur, das man vor der ersten Sicherung von Borg auf dem Backupdatenträger einrichten lässt. Für jedes angestoßene Backup legt Borg im Repository einen Datensatz an, der als Archiv bezeichnet wird. Ein Borg-Archiv ist aber anders als etwa ein Zip-Archiv keine separate Datei, sondern ein logischer Datensatz im Repository. Zur Verwaltung der Datenblöcke, Dateien und Archive verwendet Borg ähnliche Techniken wie die Versionsverwaltung Git.

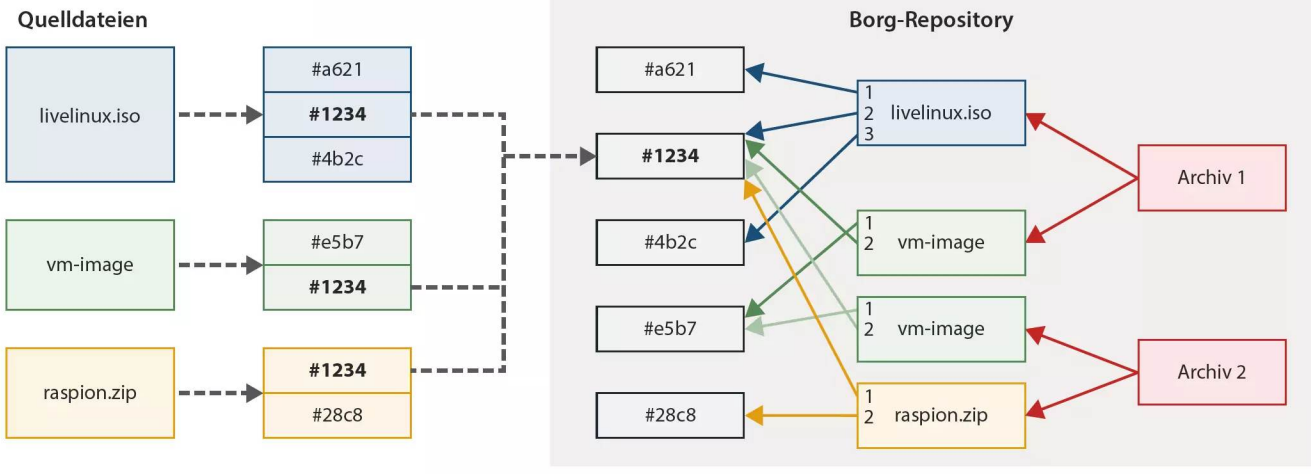
Borg dampft die ihm anvertrauten Dateien massiv ein. Dazu unterteilt es zunächst jede Datei in mehrere Blöcke. Ein Block landet nur dann im Backup, wenn es im Repository noch keinen identischen Block gibt. Über eine clevere Buchführung merkt sich Borg, welche Datenblöcke im Repository zu welchen Archiven und Dateien gehören. So spart Borg nicht nur bei zwei identischen Dateien Speicherplatz, sondern auch bei jenen, die sich ähneln. Dieses Verfahren heißt blockweise Deduplikation.

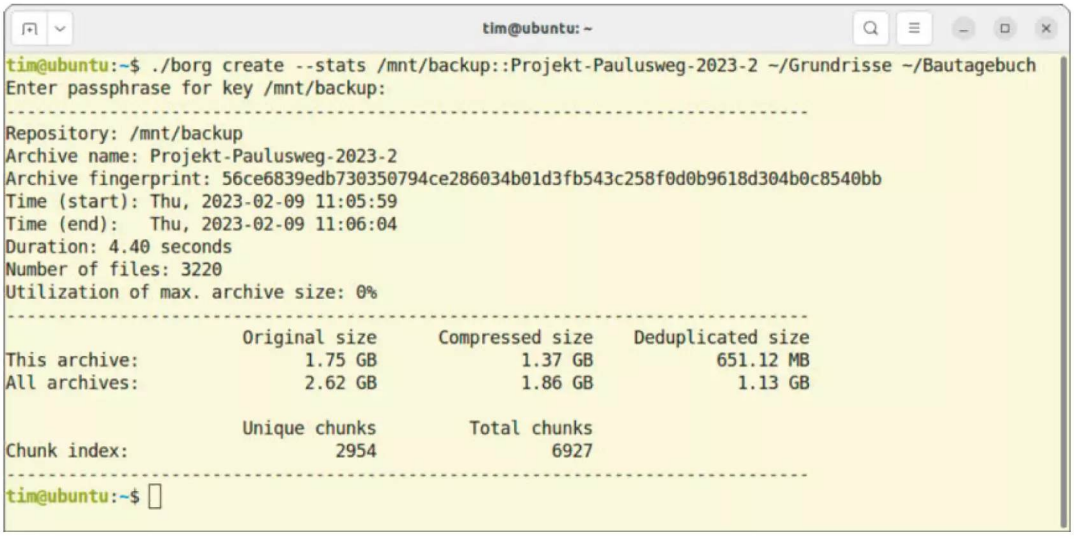
Ganz nebenbei landen bei weiteren Sicherungen nur geänderte Datenblöcke im Backup. Hat man beispielsweise eine mehrere GByte große Imagedatei für eine virtuelle Maschine gesichert und danach ändert sich die Datei nur um einige Hundert MByte, so ergänzt Borg bei der nächsten Sicherung nur die veränderten Blöcke im Repository. Da Borg dadurch gleichzeitig weniger Daten auf den Backupdatenträger schreiben muss, läuft das Backup auch schneller durch. Zudem komprimiert Borg die Datenblöcke mit einem von derzeit vier wählbaren Verfahren. Diese umfassende Schrumpfkur spart nicht nur Speicher, sondern auch Transfervolumen, wenn Sie das Backup auf einen Server oder in die Cloud hochladen.

Da nur Änderungen gesichert werden, erinnert das Vorgehen an eine inkrementelle Sicherung. Aber durch die spezielle Arbeitsweise von Borg ist jedes Archiv logisch gesehen immer ein Vollbackup. Denn ein Archiv ist eine Liste von Verweisen auf Dateiobjekte, die wiederum auf die benötigten Datenblöcke zeigen. Deshalb kann man das Repository beliebig um einzelne Archive ausdünnen, ohne dadurch spätere Sicherungspunkte unbrauchbar zu machen.

So spart das Borg-Repository Speicherplatz

Borg zerteilt die Dateien in mehrere Datenblöcke und berechnet für jeden dieser sogenannten Chunks eine Prüfsumme. Sofern es im Repository schon einen Chunk mit der gleichen Prüfsumme gibt, speichert ihn Borg nicht noch einmal, wie im Beispiel den Chunk mit der Prüfsumme #1234. Welche Chunks zu welchen Dateien gehören, merkt sich Borg in einer ausgeklügelten Datenstruktur.





Im Abschlussbericht gibt BorgBackup Auskunft, wie viel Platz Deduplikation und Kompression beim Backup einsparen.

Diese Flexibilität und den Platzgewinn erkauft man sich durch fehlende Redundanz: Sollte ein Datenblock im Backup beschädigt sein, sind automatisch auch alle darauf verweisenden Dateien betroffen – und zwar über alle Archive hinweg. Daher ist es bei BorgBackup wichtig, die zu sichernden Daten in mehreren unterschiedlichen Repositories zu sichern (siehe Kasten „3-2-1 Backups mit Borg“ auf S. 111).

Installation

Borg läuft unter Linux, macOS und einigen BSD-Systemen. Unter Linux und BSD installieren Sie Borg über die Softwareverwaltung Ihrer Distribution – meist heißt das Paket „borgbackup“. Alternativ stellt das Borg-Team die jeweils aktuelle Version als fertiges Programm bereit. Die Links zu den Downloads finden Sie auf ct.de/w9s1. Die Entwickler pflegen derzeit nicht nur die aktuelle Versionsreihe 1.2, sondern arbeiten bereits am Nachfolger Borg 2.0. Dessen Erscheinungstermin steht noch nicht fest. Von den Vorabversionen raten wir außer zu Testzwecken ab.

Um Ihre Daten zu sichern, muss das Backupmedium über einen Unix-Pfad erreichbar sein. Das dortige Dateisystem spielt für Borg fast keine Rolle: Es muss mit langen Dateinamen umgehen können und Dateien mit mehr als 2 GByte Größe aufnehmen. Die Borg-Entwickler raten zu einem Journaling-Dateisystem. Unterstützt das Dateisystem Hardlinks, nutzt sie das Backup-Tool bei einigen Operationen.

Ergänzend merkt sich Borg im Heimatverzeichnis unter „~/.cache/borg“ einige Dateisysteminformationen über die bereits gesicherten Dateien, wie etwa deren Dateigröße. Damit kann Borg später schneller geänderte Dateien finden und deduplizieren. Bei umfangreichen Repositories wächst der Cache mehrere GByte an, weshalb auf der Partition mit diesem Verzeichnis immer mehrere GByte frei sein sollten. Zudem speichert Borg für die Verschlüsselung der Repositories wichtige Dateien unter „~/.config/borg/“.

Mit Zielen im Netzwerk spricht Borg nur, wenn diese über SSH erreichbar sind und dort ebenfalls Borg installiert ist, dafür aber effizient (siehe Kasten „Outsourcing: Borg mit SSH“ auf S. 114). Um dennoch andere Netzwerkspeicher mit Borg zu verwenden, müssen Sie diese über ein Netzwerkdateisystem wie SMB oder NFS auf Ihrem System einhängen, sodass Borg über einen Unix-Pfad darauf zugreifen kann.

Backup initialisieren

In den folgenden Beispielen ist das Backupmedium unter „/mnt“ eingehängt und die Backups landen im Borg-Repository unter „/mnt/backup“. Das ist entweder ein leeres Verzeichnis, oder – falls nicht vorhanden – es wird von Borg angelegt. Damit im Repository-Verzeichnis kein Dateirechte-Chaos ent-

steht, sollten Sie alle Borg-Befehle immer unter dem gleichen Benutzerkonto aufrufen.

Mit dem folgenden Befehl erzeugen Sie unter „/mnt/backup“ ein verschlüsseltes Repository:

```
borg init --encryption=repokey /mnt/backup
```

Sie müssen sich jetzt eine Passphrase ausdenken und eintippen. Beim Initialisieren des Repository generiert Borg automatisch einen Schlüssel, mit dem es die Daten im Repository verschlüsselt. Diesen Schlüssel sichert Borg wiederum mit der Passphrase. An Ihre Backups gelangen Sie später nur mit der Kombination aus Schlüssel und Passphrase. Durch den Parameter `--encryption=repokey` speichert Borg den Schlüssel direkt im Repository. Dies hat den Vorteil, dass Sie später beim Zugriff auf das Repository immer nur die Passphrase eintippen müssen.

Borg verwendet zum Verschlüsseln und Authentifizieren die Verfahren AES-CTR-256 sowie HMAC-SHA256. Dieses Hashverfahren berechnen moderne Prozessoren mit SHA-Erweiterung hardwarebeschleunigt. Das trifft auf ARM-CPUs, AMD Ryzen und Intel Core-i ab der 10. Generation zu, sowie Atom-CPUs seit 2017 (Goldmont). Falls Ihre CPU den SHA256-Algorithmus zu langsam berechnet, kann Borg auch das konkurrierende Blake2-Verfahren verwenden. Dazu tauschen Sie im obigen Befehl „repokey“ gegen „repokey-blake2“ aus. Alle genannten Verfahren sind gut erforscht und gelten als sicher.

Um den Schlüssel bei einem Defekt des Repository wiederherstellen zu können, sollten Sie ihn in eine Datei exportieren und diese an einem sicheren Ort verwahren. Der Befehl

```
borg key export /mnt/backup > key.txt
```

sichert den Schlüssel in der Datei „key.txt“. Im Fall der Fälle stellen Sie mit

```
borg key import /mnt/backup key.txt
```

den Schlüssel wieder her.

Erstes Backup

Borg geht davon aus, dass während eines laufenden Backups niemand die zu sichernden Dateien verändert. Stoppen Sie daher vor dem Backup beson-

3-2-1-Backups mit Borg

Sichere Backups folgen der 3-2-1-Regel: Drei Kopien auf mindestens zwei verschiedenen Datenträgern, wovon eine Sicherung außer Haus lagert. Auf diese Weise haben Sie auch nach einer Überschwemmung noch ein funktionierendes Backup. Die Regel ist aber auch wichtig, da das auf Speicherplatzgröße optimierte Borg-Repository selbst keine Redundanz vorsieht.

Um die 3-2-1-Regel mit Borg umzusetzen, benötigen Sie mindestens zwei, besser drei separate Repositories – pro Speichermedium jeweils eins. Diese können sich auf einer externen Festplatte, einem NAS und – für das Außer-Haus-Backup – auf einem angemieteten Fileserver befinden.

Mounten Sie alle Speicherorte (Ausnahme: Backupserver mit Borg, siehe Kasten „Outsourcing: Borg mit SSH“ auf S. 114). Erstellen Sie dann mit `borg init` auf jedem Ziel ein eigenes Repository. Fortan speichern Sie alle anstehenden Backups in jedem der drei Repositories. Sie müssen folglich den Befehl `borg create` dreimal aufrufen, jeweils mit einem anderen Repository als Ziel. Entweder verwenden Sie für jedes Ziel einen eigenen Turnus oder Sie starten die Sicherungen nacheinander, etwa über ein Shell-Skript.

Widerstehen Sie der Versuchung, nur ein Backup-Repository zu erstellen und dieses auf die anderen Datenträger zu kopieren. Technisch geht dies zwar, aber sollte das Repository defekt sein, sind es automatisch auch die Duplikate.

Die Borg-Entwickler raten zudem davon ab, die Dateien von mehreren Systemen im gleichen Repository zu sichern, da es zum einen das von Borg verwendete Sicherheitsmodell schwächt. Zum anderen sind die Caches auf den einzelnen Rechnern nicht synchronisiert, weshalb Borg die darin befindlichen Daten häufiger und zeitraubend neu generieren müsste.

ders Anwendungen, die geöffnete Dateien in einen inkonsistenten Zustand versetzen. Halten Sie beispielsweise ein Datenbankprogramm an, bevor Sie eine Datenbank sichern. Anschließend können Sie Ihre Daten im Backup-Repository verstauen.

Der folgende Befehl sichert im Repository unter „/mnt/backup“ die Inhalte der Verzeichnisse „~/vm“ und „~/iso“ als Archiv mit dem Namen „Daten-23-01“:

```
borg create /mnt/backup::Daten-23-01 ~/vm ~/iso
```

Das Verzeichnis zum Repository sowie den Namen des Archivs fasst Borg mit zwei Doppelpunkten zu einer Pfadangabe zusammen. Alle zu sichernden Ordner und Dateien erwartet Borg hinter dem Pfad.

Von sich aus ist Borg wortkarg. Um über den Arbeitsfortschritt informiert zu werden, hängen Sie hinter `create` die Option `--progress` an. Mit `--list` protokolliert Borg die gesicherten Dateien und `--stats` generiert einen Abschlussbericht.

Den Archivnamen können Sie beliebig wählen, er muss lediglich einzigartig sein. Um die einzelnen Archive besser auseinanderzuhalten, hilft es, das Erstellungsdatum in den Namen aufzunehmen. Borg bietet dafür den Platzhalter „{now}“, den es automatisch durch das aktuelle Datum samt Uhrzeit ersetzt. Analog gibt es noch die Platzhalter „{hostname}“ für den Rechner- und „{user}“ für Ihren Benutzernamen:

```
borg create /mnt/backup::Backup-{hostname}-↵
                      ↳{user}-{now} ~/vm  ~/iso
```

Jede weitere Sicherung, die Sie mit `borg create` anlegen, landet in einem eigenen Archiv. Welche Verzeichnisse und Dateien Sie dabei in den Archiven speichern, bleibt Ihnen überlassen. Wenn Sie allerdings in jedem Archiv andere Daten ablegen, geht recht schnell die Übersicht verloren. Sie sollten daher diszipliniert in jedem Repository immer die gleichen Daten sammeln, etwa ihr Home-Verzeichnis oder das gleiche Projektverzeichnis. Damit kann auch die Deduplikation effizientere Ergebnisse liefern.

Dateien ausschließen

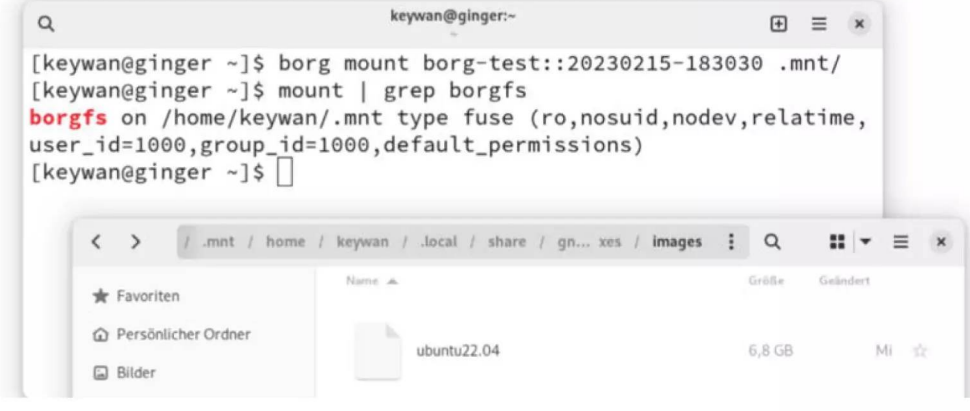
Um einzelne Dateien oder Unterordner vom Backup auszuschließen, verwenden Sie den Schalter `--exclude`, gefolgt vom vollständigen Datei- oder Verzeichnispfad. Mehrere Dateien schließen Sie entweder über weitere `--exclude` aus oder nutzen Wildcards. Das folgende Beispiel ignoriert sämtliche Dateien mit der Endung „.tmp“, sowie das Verzeichnis „~/vm/.cache/

```
borg create --exclude '*.tmp' --exclude ↵
    ↳~/vm/.cache/ /mnt/backup::Projekt-{now} ~/vm
```

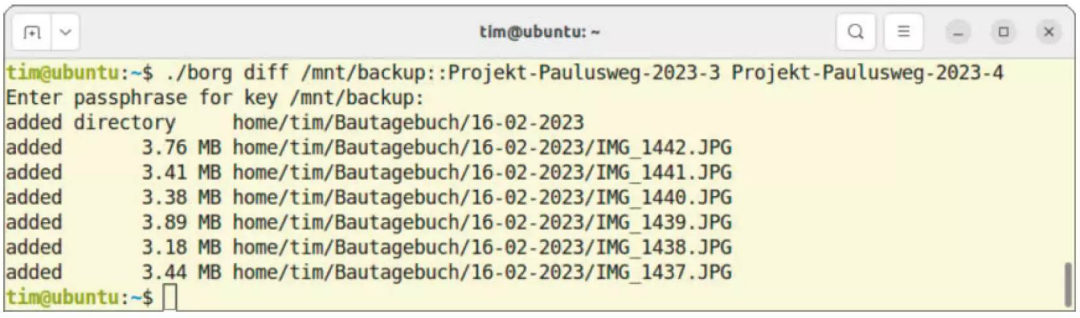
Borg durchläuft bei der Sicherung sämtliche Unterordner. Sollte dort irgendwo ein USB-Stick oder Netzlaufwerk eingehängt sein, sichert Borg dessen Inhalte mit. Sie verhindern dies mit `--one-file-system`, da Borg dann nicht in ein anderes Dateisystem wechselt. Die Erkennung hat ihre Grenzen, da es beispielsweise Btrfs-Subvolumes als eigene Dateisysteme ansieht.

Backup komprimieren

Üblicherweise komprimiert Borg die Datenblöcke mit dem LZ4-Algorithmus. Der arbeitet zwar recht



BorgBackup hängt Backuparchive als virtuelles Laufwerk ein, die man dann mit einem beliebigen Dateimanager durchsuchen kann.



Mit diff listet Borg-Backup den Unterschied zwischen zwei Archiven auf.

flott, schrumpft aber weniger effektiv als Zstandard (Zstd). Sie wechseln das Verfahren mit der Option `--compression`. Der Befehl

```
borg create --compression zstd
```

komprimiert die Daten mit Zstd. Laut Borg-Dokumentation eignet sich Zstd für die meisten Daten, wobei LZ4 schneller ist als gar keine Kompression (`--compression none`), da Borg weniger Daten auf das Backupmedium schreiben muss. Für die Rückwärtskompatibilität mit älteren Versionen unterstützt Borg auch noch Zlib und LZMA. Bei bereits stark komprimierten Dateien wie Zip-Archiven oder Videos lohnt sich meist keine Kompression. Mit der Option `--compression auto,zstd` weisen Sie Borg an, nur mit dem angegebenen Verfahren (hier Zstd) zu komprimieren, wenn Borg es für sinnvoll hält.

Backup überprüfen und wiederherstellen

Um sich einen Überblick über die im Repository enthaltenen Archive zu verschaffen, rufen Sie `borg list /mnt/backup` auf. Ergänzen Sie dahinter den Archivnamen, um die darunter gespeicherten Dateien und Verzeichnisse aufzulisten:

```
borg list /mnt/backup::Daten-23-01
```

Um nur einen Teil des Archivs anzuzeigen, hängen Sie den Pfad zu den gesuchten Verzeichnissen oder Dateien an.

Den Unterschied zwischen zwei Archiven erledigt `borg diff` gefolgt von den Namen der beiden Archive. Das folgende Beispiel vergleicht die Inhalte im Archiv „Daten-23-01“ mit denen aus dem Archiv „Daten-23-02“, die beide im Repository „/mnt/backup“ liegen:

```
borg diff /mnt/backup::Daten-23-01 Daten-23-02
```

Auch bei `diff` grenzen Sie die Ausgabe auf bestimmte Dateien oder Verzeichnisse ein, wenn Sie hinter den Archivnamen einen Pfad anhängen.

Möchten Sie zunächst nur in einem Archiv stöbern, mounten Sie es als virtuellen Datenträger. Folgender Befehl braucht keine Root-Rechte und hängt das Archiv „Projekt-23-01“ in das vorhandene Verzeichnis „~/content“ ein.

```
borg mount /mnt/backup::Daten-23-01 ~/content
```

Anschließend haben Sie unter „~/content“ schreibgeschützten Zugriff auf alle Archivinhalte. Von dort können Sie alle Dateien wie gewohnt öffnen und kopieren. Die Archive hängt Borg mithilfe von FUSE (**F**ilesystem in **Use**rspace) ein, was sich ebenfalls auf Ihrem System befinden muss. Bei vielen Linux-Distributionen wird es mitinstalliert. Nach getaner Arbeit hängen Sie mit `borg unmount ~/content` das Archiv wieder aus.

Um alle Daten aus einem Archiv wiederherzustellen, wechseln Sie zunächst in ein leeres Verzeichnis, denn Borg überschreibt vorhandene Dateien. Setzen Sie aus diesem Verzeichnis heraus dann `borg extract` auf das Archiv an:

```
cd ~/restore
borg extract /mnt/backup::Daten-23-01
```

Dieser Befehl entpackt den kompletten Inhalt des Archivs „Projekt-23-01“ in das Verzeichnis „~/restore“. Borg restauriert dabei neben den Pfaden auch die Zugriffsrechte und Zeitstempel. Stoßen Sie die Wiederherstellung möglichst mit dem Benutzerkonto an, mit dem Sie auch die Sicherung durchgeführt haben.

Mit dem Kommando `borg check --info /mnt/backup` prüfen Sie, ob das Repository unter Bitfäule oder anderen Defekten leidet. Die Dauer der Prüfung hängt von der Repository-Größe ab. Meldet Borg ein defektes Repository, räumen Sie zunächst einen Hardware-Defekt (zum Beispiel RAM, SSD oder Festplatte) aus.

Borg kann das Repository auch reparieren, was aber Grenzen hat. Ist ein Datenblock beschädigt oder fehlt er, merkt sich die Reparaturfunktion dessen ID und ersetzt die Verweise zu einem gleichgroßen Block, der nur aus Nullen besteht. Erzeugt ein späteres Backup wieder einen Block mit dieser ID, heilt Borg die defekten Dateien wieder, indem es die Verweise vom Nullblock auf den wiederentdeckten korrekten Block zurückändert. Da nicht ausgeschlossen ist, dass die Reparatur das Repository zusätzlich beschädigt, empfehlen die Borg-Entwickler, das Repository vorher zu kopieren. Für die Reparatur rufen Sie `borg check --repair` auf. Stoßen Sie danach, sollten die Originaldateien noch vorhanden sein, eine neue Sicherung an.

Backups aufräumen

Geht der Speicherplatz auf dem Backupdatenträger zur Neige, löschen Sie nicht mehr benötigte Archive mit `borg delete`. Anschließend müssen Sie

Outsourcing: Borg mit SSH

Wenn auf einem Server mit SSH-Zugang ebenfalls Borg installiert ist, arbeitet das Backup-Tool effizienter. Das lokal laufende Borg kümmert sich weiter um Deduplikation, Kompression, Verschlüsselung und verwaltet die Archive, während es Low-Level-Aktionen an `borg serve` delegiert. Das holt unter anderem Datenblöcke aus dem Repository oder fügt neue hinzu und wendet Befehle wie `check` oder `compact` an. Dadurch minimiert Borg die Datenmenge, die übers Netzwerk übertragen werden muss.

Um so auf ein entferntes Repository zuzugreifen, ergänzen Sie den Pfad, indem Sie den Benutzer- und Hostnamen für die SSH-Verbindung voranstellen:

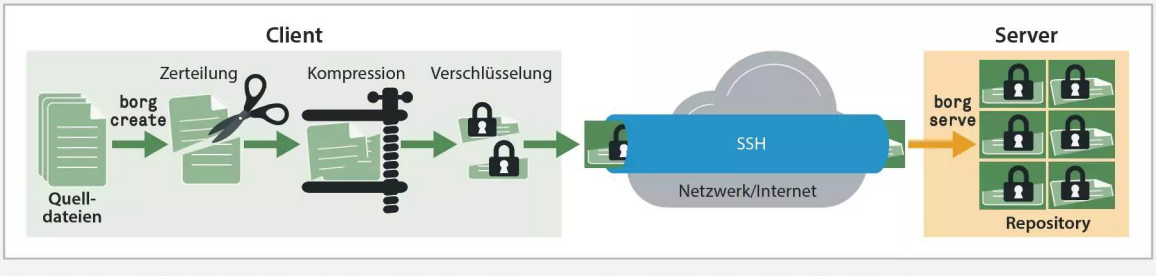
```
borg init --encryption=repokey ↵
        ↳tim@wolke.local:/mnt/backup
```

Hier meldet sich Borg per SSH beim Server wolke.local als Benutzer „tim“ an und richtet dort im Verzeichnis /mnt/backup ein Repository ein.

Wollen Sie den durch AES und Ihre Passphrase geschützten Schlüssel partout nicht auf dem Server im Repository lagern, können Sie den Schlüssel lokal in einem separaten Keyfile speichern. Initialisieren Sie dazu das Repository mit `--encryption=keyfile`. Borg speichert dann den Schlüssel auf Ihrem Rechner im Verzeichnis „~/.config/borg/keys“.

Falls Sie selber keinen SSH-Server mit Borg aufsetzen wollen, können Sie auch einen mieten. Anbieter wie BorgBase, Rsync.net oder Hetzner stellen auf Borg zugeschnittene Cloudspeicher bereit.

Verstopft das Backup beim Upload Ihre Netzwerkleitung, drosseln Sie die Datenrate mit `--upload-ratelimit`. Als Wert geben Sie das gewünschte Limit in KByte/s an, zum Beispiel 1000.



BorgBackup teilt die Arbeit zwischen Client und Server auf, um beim Zugriff auf entfernten Repositories Datentransfer zu minimieren.

noch `borg compact` aufrufen, damit Borg die nicht mehr benötigten Datenblöcke entfernt. Aufgrund der Deduplikation lässt sich meist nicht zuverlässig vorhersagen, wie viel Speicherplatz freigegeben wird.

Statt händisch einzelne Archive zu löschen, entfernt `borg prune` automatisch ältere Archive. Mit folgendem Befehl behält Borg alle in den letzten 24 Stunden erstellten Archive (`--keep-within=1d`) sowie jeweils das jüngste Backup für die letzten sieben Tage (`--keep-daily=7`):

```
borg prune --list --dry-run --keep-within=1d ⮦
    ↳--keep-daily=7 /mnt/backup
```

Mit `--dry-run` simuliert Borg den Vorgang und listet Ihnen nur auf, welche Archive es löschen würde. Wenn die Liste stimmt, rufen Sie den Befehl ohne `--dry-run` auf. Anschließend geben Sie mit `borg compact` den Speicherplatz frei.

Borg per Skript steuern

Als Kommandozeilen-Tool können Sie Borg sehr einfach in eigene Skripte einbinden, worauf es zusätzlich optimiert ist. Stellen Sie den Pfad zum Repository über die Umgebungsvariable `BORG_REPO` bereit, um die Pfadangabe bei den einzelnen Kommandos einzusparen.

```
#!/bin/bash
export BORG_REPO="/mnt/backup"
borg create ::{now} ~/Daten
```

Auch die Passphrase können Sie mit der Umgebungsvariable `BORG_PASSPHRASE` übergeben. Möchten Sie vermeiden, dass die Passphrase als Klartext im Hauptspeicher steht, verwenden Sie stattdessen `BORG_PASSCOMMAND`. Darin definieren Sie einen Befehl, über den Borg das Passwort über ein externes Programm wie gpg oder einen Passwortmanager abruft. Alternativ können Sie mit `BORG_PASSPHRASE_FD` auch einen File-Deskriptor angeben, über den Borg die Passphrase einliest. Borg kennt noch weitere spezifische Umgebungsvariablen. Den Link zur Dokumentation finden Sie unter ct.de/w9s1.

Die zu sichernden Daten nimmt `borg create` auch über die Standardeingabe entgegen. Nutzt man dazu, wie von anderen Shell-Befehlen gewohnt, einen angehängten Bindestrich (`-`), speichert Borg den empfangenen Datenstrom als eigene Datei im Repository. Damit Borg die Eingabe als Pfade der zu sichernden Dateien und Verzeichnisse interpretiert, verwenden Sie die Option `--paths-from-stdin` (ohne `-` am Ende). Mit `--paths-from-command` (oder `--contents-from-command`) ruft Borg selbst das Programm auf und legt ein neues Archiv nur dann an, wenn das externe Kommando erfolgreich durchlief.

Borg gibt die bekannten Fehlercodes aus: Bei `0` gab es keine Probleme, `1` steht für einen mit Warnungen beendeten Durchlauf von Borg und bei `2` verursachte ein Fehler einen vorzeitigen Abbruch. Um Fehler zu analysieren, ergänzen Sie die Optionen `--info` (kurz `-v`) oder `--debug`. Alle Protokollausgaben schickt Borg über Standardfehlerausgabe (`stderr`) raus – auch die von `--stats` und `--list`.

Über mehrere Wege gibt Borg Informationen im strukturierten JSON-Format aus, was waghalsige Mustererkennungen der Textausgabe erspart. Die Option `--json` gibt den Output von Subkommandos wie `info`, `create`, `diff` oder `list` als ein JSON-Objekt auf der Standardausgabe (`stdout`) wieder, die Sie mit dem Programm `jq` oder JSON-Bibliotheken weiterverarbeiten können. Bei `create` beschränkt sich `--json` auf den Abschlussbericht (`--stats`) und `borg list` akzeptiert es nur für Repository-Inhalte. Für die Ausgabe der Archivinhalte verwenden Sie stattdessen `--json-lines`. Die Option kennt auch `diff` und spuckt pro Zeile ein separates JSON-Objekt aus. So verschlucken sich bei langen Listen die Interpreter nicht an zu großen JSON-Objekten.

Um Fehlermeldungen, Warnungen oder die Ausgabe von `create --list` im JSON-Format zu bekommen, verwenden Sie `--log-json`. Deren JSON-Ausgaben landen weiterhin auf der Standardfehlerausgabe. Die Details zur Datenstruktur und Sonderfälle beschreibt die Borg-Dokumentation (siehe ct.de/w9s1).

Die durchdachten Schnittstellen von Borg eignen sich nicht nur dafür, über eigene Skripte die lästige Datensicherung zu automatisieren, sondern auch regelmäßig automatisch zu prüfen, ob die Backups noch heil sind.

Weitere Hilfen

Borg bietet noch viel mehr Optionen, die in der ausführlichen Onlinedokumentation erläutert sind. Dort finden Sie Beschreibungen von verschiedenen Szenarien für Borg, etwa das Hosting von Borg-Repositories für mehrere Benutzer. Die recht einfache Arbeitsweise von BorgBackup erweist sich in der Praxis als äußerst flexibel und leistungsfähig. (ktn) c't

Downloads und Borg-Dokumentation

ct.de/w9s1

Gelöschte Dateien wiederherstellen

Noch schnell vor dem Feierabend die Festplatte des Linux-Rechners aufgeräumt – und schon hat man die falsche Datei mit der Arbeit des ganzen Tags gelöscht. Wenn Sie schnell und besonnen reagieren, stehen beim Dateisystem Ext4 die Chancen gut, Ihre Daten wiederzubekommen.

Von **Mirko Dölle**

Weg ist weg: Wenn man unter Linux eine Datei löscht, dann ist dies normalerweise ziemlich endgültig. Grafische Dateimanager wie Nautilus von Gnome verschieben die Dateien zunächst in den Papierkorb – doch ist der geleert, wird es kompliziert. Der Grund dafür liegt darin, wie das Standarddateisystem Ext4 Dateien löscht: Anstatt wie im FAT-Dateisystem die Datei lediglich als gelöscht zu markieren und die von der Datei belegten Datenblöcke freizugeben, überschreibt Ext4 die obere Ebene der Blockzuordnung im Verwaltungsblock der Datei, dem Inode, sodass sich die zur Datei gehörenden Datenblöcke nicht mehr ermitteln lassen. Allerdings wird diese Änderung im Journal des Dateisystems aufgezeichnet, sodass es einen Weg zurück gibt, solange das Journal fortbesteht.

Es kommt also darauf an, schnell zu handeln, um das Journal zu retten und zu verhindern, dass die freigegebenen Datenblöcke der gelöschten Datei

überschrieben werden. Sie sollten sich deshalb diesen Artikel gut aufheben oder ein Lesezeichen im Browser oder in der App setzen, damit Sie die „To-do-Liste für gelöschte Dateien“ im Notfall sofort zur Hand haben und Schritt für Schritt abhaken können. Anschließend haben Sie Zeit, sich in Ruhe damit auseinanderzusetzen, wie Sie Ihre Daten zurückbekommen.

Doppelte Buchführung

Das Journal ist bei Ext4 eigentlich dafür gedacht, nach einem Absturz oder Stromausfall einen konsistenten Dateisystemzustand wiederherzustellen. Dazu werden Dateisystemänderungen erst im Journal aufgezeichnet, umgesetzt und dann im Journal als erledigt markiert. Welche Daten im Journal landen, bestimmt die Mount-Option `data=`: In der Standardeinstellung `data=ordered` werden Nutzdaten direkt in die Datenblöcke geschrieben, das Journal protokolliert anschließend nur Verwaltungsinformationen.

Dieser Modus ist bedeutend schneller als die doppelte Buchführung von `data=journal`, bei der auch die Nutzdaten zunächst im Journal landen, bevor sie in die Datenblöcke kopiert und schließlich die Verwaltungsinformationen angepasst werden. Am schnellsten ist der Modus `data=writeback`, hier werden Nutzdaten und Metadaten parallel geschrieben – was aber das Risiko für Inkonsistenzen erhöht, da möglicherweise eine Schreiboperation nicht vollständig ausgeführt, die Änderungen aber bereits im Journal erfasst wurden.

Bei den Verwaltungsinformationen, auch Metadaten genannt, handelt es sich zum Beispiel um einen Verweis auf die Liste der Datenblöcke, die zu einer Datei gehören, aber auch ihre Dateirechte und wann der letzte Zugriff erfolgte. Diese werden im Inode aufbewahrt, den jede Datei, aber auch jedes Verzeichnis besitzt. Jede Veränderung dieser Verwaltungsinformationen, etwa weil eine Datei vergrößert wird und deshalb neue Datenblöcke hinzukommen, zeichnet das Ext4-Dateisystem im Journal auf.

Auch wenn Sie eine Datei oder ein Verzeichnis rekursiv löschen, protokolliert Ext4 dies im Journal. Genau diesen Umstand nutzt das Dateisystem-Tool ext4magic: Es liest das Journal und kann Dateien wiederherstellen, indem es gewissermaßen das Journal dieser Datei zurückspult. Allerdings wird das Journal rollierend genutzt – sobald es voll ist, werden die ältesten Protokolldaten überschrieben. Wie groß das Journal auf Ihrem Rechner ist, finden Sie mit folgendem Befehl im Terminal heraus:

```
sudo dumpe2fs /dev/sda3 |grep Journal
```

To-do-Liste für gelöschte Dateien

1. Papierkorb kontrollieren: Grafische Dateimanager löschen die Dateien meist nicht direkt.
2. RAM-Dateisystem unter /mnt einbinden, um darauf das Journal ohne Beeinflussung des Root-Dateisystems zwischenzuspeichern: `sudo mount -t tmpfs tmpfs /mnt`
3. Angeschlossene Laufwerke und ihre Mount-Points auflisten lassen, um den Gerätenamen des betroffenen Dateisystems herauszufinden: `lsblk -fp`
4. Größe und Inode-Nummer des Ext4-Journals ermitteln (Standard: 1 GByte, Inode 8): `sudo dumpe2fs /dev/sda3 | grep Journal` Dabei müssen Sie den Gerätenamen (`/dev/sda3`) gemäß der Ausgabe von `lsblk` aus dem vorherigen Schritt anpassen. Bei verschlüsselten Ubuntu-Installationen lautet der Gerätename des Root-Dateisystems zum Beispiel `/dev/mapper/vgubuntu-root`.
5. Ausstehende Dateioperationen abschließen lassen und das Journal im RAM-Dateisystem speichern: `sync && debugfs -R "dump <8> /mnt/ext4.journal" /dev/sda3`. Die Inode-Nummer (`<8>`) ist Standard, kann im Einzelfall aber abweichen – die korrekte Inode-Nummer finden Sie in der Ausgabe des vorherigen Schritts.
6. Journalkopie /mnt/ext4.journal auf einen (externen) Datenträger, NAS oder per `scp` auf einen anderen Rechner kopieren.
7. Rechner ausschalten und Festplatte ausbauen oder mit Livesystem starten, bis die Daten wiederhergestellt sind.

Den Gerätenamen `/dev/sda3` müssen Sie selbstverständlich anpassen. Welche Dateisysteme wo eingebunden sind und auf welchen Geräten sie liegen, erfahren Sie mit dem Befehl `lsblk -fp`. Bei SSDs könnte der Gerätename auch /dev/nvme0n1p3 lauten; wenn Sie ein verschlüsseltes Dateisystem oder LVM benutzen, dann liegt das Gerät unterhalb des Verzeichnisses /dev/mapper. Bei Ubuntu etwa ist der Gerätename des Root-Dateisystems üblicherweise /dev/mapper/vgubuntu-root, bei Debian ist der Hostname im Gerätenamen enthalten, Standard ist dort /dev/mapper/debian--vg-root. Lassen Sie sich also nicht von ungewöhnlichen Gerätenamen abschrecken.

Zusätzlich kontrolliert der Dateisystemtreiber beim Einhängen eines Ext4-Dateisystems, ob alle Aktionen im Journal auch ausgeführt wurden – falls nicht, holt er die noch ausstehenden Operationen nach – und löscht schließlich das alte Journal. Damit ext4magic eine Chance hat, gelöschte Dateien wiederherzustellen, dürfen Sie also nicht den Rechner neu starten und Sie müssen hoffen, dass die Löschoperation im Journal nicht durch weitere Dateisystemoperationen überschrieben wird.

Schnell in Sicherheit

Der erste Schritt zur Datenrettung ist, dass Sie so schnell wie möglich eine Kopie des Journals anlegen und das Tool ext4magic später mit dem Journal-Backup arbeiten lassen. Diese Kopie dürfen Sie nicht auf dem Dateisystem der gelöschten Datei speichern, zu groß ist die Gefahr, dass dabei die zu rettenden Datenblöcke überschrieben werden. Eine andere Festplattenpartition, ein USB-Stick oder eine externe SSD sind ideale Aufbewahrungsorte – wenn man diese denn zur Hand hat. Falls nicht, können Sie das Journal einfach auf einer RAM-Disk zwischenspeichern: Diese ist immer verfügbar und es verschafft Ihnen Zeit, anschließend in Ruhe nach einem dauerhaften Datenträger zu suchen. Die einzige Voraussetzung ist, dass Sie noch etwa 1 GByte freien RAM haben – einschließlich Swap-Partition, auch dort ist die Journalkopie vorerst gut aufgehoben.

Die Größe der RAM-Disk müssen Sie nicht spezifizieren, sondern lediglich den Einhängepunkt – wir empfehlen das Verzeichnis /mnt:

```
sudo mount -t tmpfs tmpfs /mnt
```

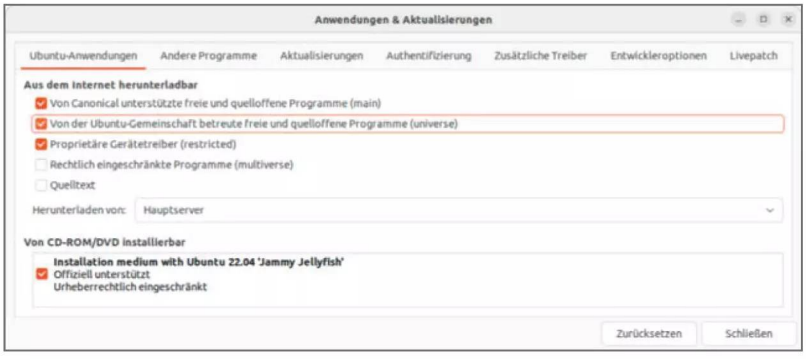
Das Programm `debugfs` erlaubt es Ihnen, Dateien im Dateisystem auch anhand des Verwaltungsblocks, dem sogenannten Inode, zu finden. Das ist beim Journal notwendig, weil es keinen Dateisystemeintrag und damit keinen Dateinamen besitzt. Welcher Inode für das Journal Ihres Dateisystems zuständig ist, haben Sie bereits im vorletzten Schritt von `dumpe2fs` unter „Journal inode“ erfahren – Standard ist Inode 8. Mit der `debugfs`-Operation `dump` kopieren Sie alle zu Inode 8 gehörenden Datenblöcke und damit das komplette Journal in die Datei `ext4.journal` auf der RAM-Disk:

```
debugfs -R "dump <8> /mnt/ext4.↵
↳journal" /dev/sda3
```

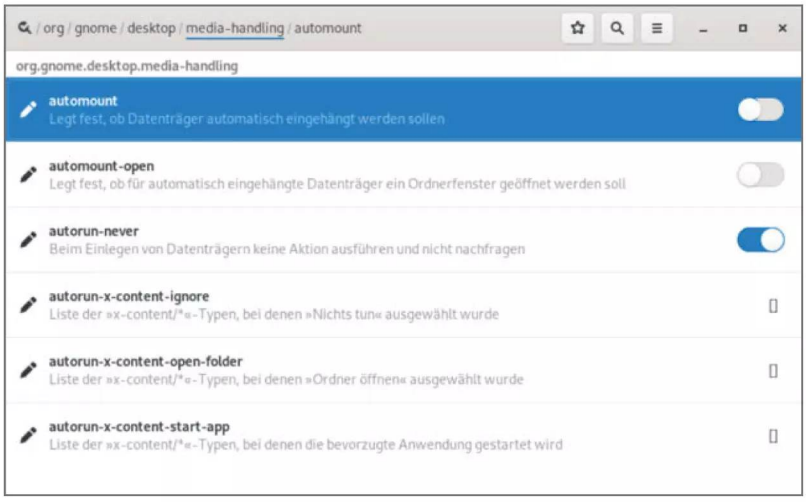
Und auch hier müssen Sie den Gerätenamen `/dev/sda3` wieder anpassen, so wie bei den Kommandos zuvor schon.

Damit ist die Kuh fast schon vom Eis, Sie können jetzt in Ruhe nach einem Datenträger für die Journalkopie suchen. Vermeiden Sie aber weiterhin, Daten auf das Dateisystem zu kopieren. Sie sollten auch vorerst möglichst wenige Programme öffnen und schließen, Browser und Mail-Programme etwa speichern viele Daten auf dem Dateisystem zwischen – je mehr verändert wird, desto größer ist die Wahrscheinlichkeit, dass zu rettende Daten dabei überschrieben werden. Haben Sie das Journal auf den Datenträger kopiert, können Sie Ihren Rechner herunterfahren und ausschalten.

Für die Wiederherstellung der Daten gibt es zwei Möglichkeiten: Sie können Ihren Rechner von einem USB-Stick mit einem Live-Linux wie Ubuntu 22.04 LTS oder dem aktuellen Desinfec’t booten, oder Sie bauen die Festplatte des Rechners aus und schlie-



In Live-Linux-Systemen wie Ubuntu 22.04 LTS sind notwendige Tools wie ext4magic und der Dconf-Editor erst verfügbar, wenn Sie zusätzliche Repositories als Paketquellen aktivieren – bei Ubuntu ist es das Universe-Repository.



Bevor Sie die Festplatte mit den wiederherzustellenden Daten an einen anderen Linux-Rechner anschließen, müssen Sie dort den Auto-Mounter deaktivieren. Andernfalls wird das Journal des Ext4-Dateisystems beim Einbinden automatisch gelöscht.

ßen sie, etwa mit einem USB-Adapter, an einen anderen Linux-Rechner an.

Besser im Handbetrieb

Die Festplatte an einen anderen Rechner anzuschließen ist tückisch, denn üblicherweise werden Wechselmedien wie externe Festplatten automatisch eingebunden – und damit das Journal gelöscht. Da Sie eine Kopie besitzen, wäre dies keine Katastrophe. Um möglichst wenige Veränderungen am Dateisystem zu provozieren, sollten Sie trotzdem den Auto-Mounter deaktivieren, bevor Sie Ihre Festplatte anschließen.

Unter Ubuntu 22.04 LTS und anderen Distributionen mit Gnome-Desktop können Sie dazu den grafischen Dconf-Editor verwenden. Dieser ist bei Ubuntu 22.04 LTS allerdings nicht im Livesystem enthalten und findet sich auch nicht in den standardmäßig aktivierten Repositories. Daher starten Sie zunächst das Programm „Anwendungen & Aktualisierungen“ und aktivieren im Reiter „Ubuntu-Anwendungen“ das Universe-Repository. Sobald Sie auf „Schließen“ klicken, lädt das Programm die Paketlisten neu, woraufhin Sie in „Ubuntu-Software“ den „Dconf-Editor“ installieren können.

Haben Sie den Dconf-Editor gestartet, hangeln Sie sich im Konfigurationsbaum nach /org/gnome/desktop/media-handling vor. Dort finden Sie die Punkte „automount“ und „automount-open“, die bereits aktiviert sind. Indem Sie beide ausschalten und dann den Dconf-Editor schließen, legen Sie den Auto-Mounter lahm.

Als Alternative zum Dconf-Editor können Sie den Auto-Mounter auch im Terminal abschalten, dazu genügen die beiden folgenden Befehle:

```
gsettings set org.gnome.desktop.↵
↳media-handling automount false
gsettings set org.gnome.desktop.↵
↳media-handling automount-open false
```

Anschließend können Sie gefahrlos den USB-Adapter mit Ihrer Festplatte anschließen.

Interne Festplatten sind keine Wechsellaufwerke und werden beim Booten der Livesysteme auch nicht automatisch eingebunden. Deshalb können Sie darauf verzichten, den Auto-Mounter zu deaktivieren, wenn Sie Ihren Rechner vom USB-Stick starten. Sie dürfen allerdings nicht im grafischen Dateimanager auf das Laufwerk klicken – sonst wird es eingebunden und dabei wird das Journal gelöscht.

Aufgeschlüsselt

Wollen Sie die Dateien einer verschlüsselten Linux-Installation retten, so beginnt ohne den Auto-Mounter eine Odyssee auf der Kommandozeile. Schließlich gibt es niemanden mehr, der die Verschlüsselung erkennt, nach dem Passwort fragt und sich, falls vorhanden, um die Logical Volume Group mit den einzelnen Volumes kümmert. Das alles müssen Sie deshalb in Handarbeit erledigen.

Los geht es damit, den verschlüsselten LUKS-Container zu öffnen. Dabei hilft Ihnen abermals der Befehl `lsblk -lp`, der Ihnen die verfügbaren Speicherlaufwerke auflistet. Tauchen in der Spalte `FSTYPE` die Begriffe `crypt`, `crypto` oder `crypto_LUKS` auf, so haben Sie es mit einer verschlüsselten Partition zu tun. Als Beispiel verwenden wir nachfolgend /dev/sda3, den Namen Ihrer Partition finden Sie am Anfang der Zeile in der Ausgabe von `lsblk`. Setzen Sie nun `cryptsetup` auf die LUKS-Partition an:

```
sudo cryptsetup open \
/dev/sda3 sda3_crypt
```

Das Programm fragt die Passphrase für die Verschlüsselung ab und stellt die entschlüsselte Partition unter `/dev/mapper/sda3_crypt` bereit. Wie es in

der verschlüsselten Partition aussieht, hängt von der Linux-Distribution ab, die sie angelegt hat: Manche wie Ubuntu und Debian legen eine LVM-Volume-Group (Logical Volume Management) in der entschlüsselten Partition an, um dort mehrere Dateisysteme nebeneinander unterzubringen.

In diesen Fällen zeigt `lsblk -fp` bei `/dev/mapper/sda3_crypt` als Dateisystemtyp `lvm`, `LVM2` oder `LVM2_member` an und Sie müssen LVM mit dem Befehl `sudo vgchange -ay` nach neuen Volume Groups suchen und sie aktivieren lassen. Die in der Volume Group enthaltenen logischen Laufwerke (Logical Volumes) werden Ihnen daraufhin mit dem Befehl `lsblk -fp` gelistet. Bei Ubuntu-Installationen heißt das Root-Dateisystem, von dem Sie gelöschte Dateien wiederherstellen, `/dev/mapper/vgubuntu-root`. Andere Distributionen verzichten auf ein LVM und verwenden stattdessen für jede Partition einen eigenen LUKS-Container, sodass Ihnen in `/dev/mapper/sda3_crypt` bereits das entschlüsselte Ext4-Dateisystem für die Datenrettung vorliegt. In den Fällen zeigt `lsblk -fp` als Dateisystemtyp `ext4` an.

Bevor Sie die Dateien entlöschen, benötigen Sie erst eine ausreichend große Datenhalde – idealerweise eine externe Festplatte oder zumindest einen USB-Stick, auf den deutlich mehr als die zu rettenden Daten passt. Ohne Auto-Mounter müssen Sie auch diese von Hand einbinden, etwa unter /mnt. Hier ein Beispielbefehl für das Laufwerk /dev/sdc1:

```
sudo mount /dev/sdc1 /mnt
```

Wie der korrekte Gerätename bei Ihrer externen Festplatte lautet, verrät Ihnen wieder einmal `lsblk -fp`, sobald Sie das Laufwerk angeschlossen haben.

Rette sich, wer kann!

Nun sind Sie endlich bereit, Ihre wertvollen Daten wiederherzustellen. Wenn Sie bisher das alte Journal ungelöscht bewahren konnten, dann ist der Aufruf von ext4magic sehr einfach. Folgender Befehl stellt alle gelöschten Dateien des Root-Dateisystems `/dev/mapper/vgubuntu-root` unterhalb von `/mnt` wieder her:

```
sudo ext4magic -m -d /mnt \
/dev/mapper/vgubuntu-root
```

Wenn Sie den Zeitpunkt eingrenzen können, wann Sie die gesuchte Datei versehentlich gelöscht haben, so können Sie diese Angabe ebenfalls ergänzen. Der Befehl

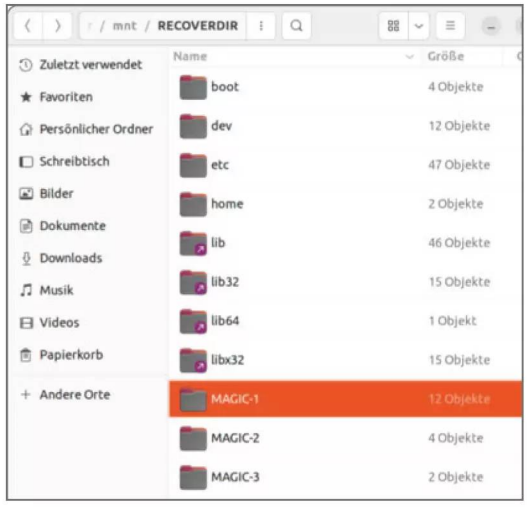
```
sudo ext4magic -m \
-a $(date -d "-2day" +%s ) \
-d /mnt /dev/mapper/vgubuntu-root
```

stellt alle Dateien wieder her, die in den vergangenen 48 Stunden gelöscht wurden. Mit dem Parameter `-b` können Sie zudem eine Obergrenze setzen; indem Sie `-b $(date -d "yesterday" +%s)` ergänzen, wählen Sie einen Zeitraum von maximal 48 Stunden bis mindestens 24 Stunden aus.

Ebenfalls praktisch ist der Parameter `-f`, mit dem Sie den Dateinamen der gesuchten Datei angeben. Das funktioniert vor allem dann, wenn Sie ganze Verzeichnisbäume gelöscht haben, aber nur einzelne Dateien benötigen oder nicht genügend Festplattenplatz für die komplette Wiederherstellung haben. Hätte der Autor sein Home-Verzeichnis versehentlich gelöscht, würde folgender Befehl diesen Artikel wiederherstellen:

```
sudo ext4magic -m -f home/mid/↵
↳Dokumente/artikel/ext4magic.txt ↵
↳-d /mnt /dev/mapper/vgubuntu-root
```

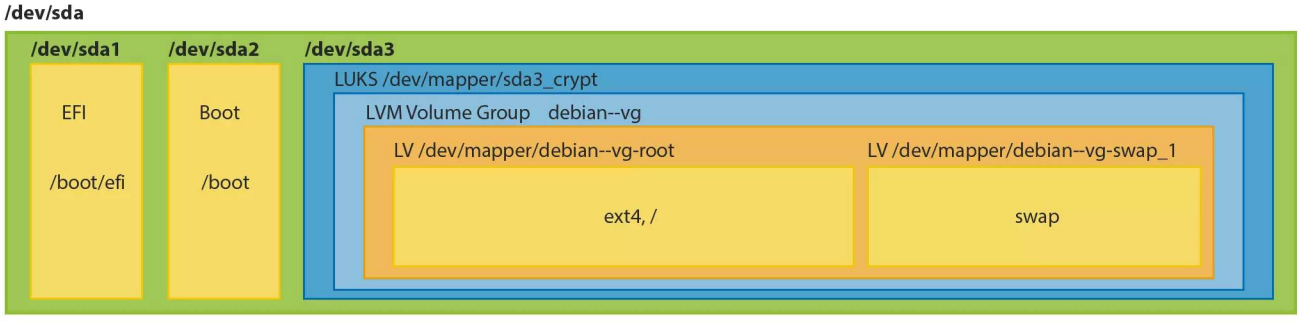
Auch dabei gibt es weitere Optionen, etwa um den Löschzeitpunkt einzugrenzen. Allerdings bleibt der Dateiname nicht immer erhalten, weshalb Sie im Zweifel lieber allein den Löschzeitpunkt verwenden oder ganz unbegrenzt wie im ersten Beispiel alle gelöschten Dateien wiederherstellen lassen sollten. ext4magic kennt auch ein Disaster-Recovery: Mit



Kann ext4magic den Namen und -pfad bestimmen, sortiert es die wiederhergestellten Dateien anhand des Originalpfads ein. In den Verzeichnissen `MAGIC-1` bis `MAGIC-3` werden die Dateinamen anhand von Inode-Nummer oder Dateityp einsortiert.

Schichtbetrieb

Ohne die Hilfe des Auto-Mounters ist es sehr aufwendig, an das Root-Dateisystem mit den gelöschten Dateien heranzukommen: Zunächst öffnen Sie die verschlüsselte Partition mit `cryptsetup`. Bei Debian und Ubuntu versteckt sich darin eine LVM Volume Group, die Sie mittels `vgchange` von Hand aktivieren müssen. Erst dann können Sie auf das Root-Dateisystem, `hier /dev/mapper/debian--vg-root`, zugreifen und mit der Datenrettung beginnen.




```
sudo ext4magic -M -d /mnt \
/dev/mapper/vgubuntu-root
```

stellt das Programm das gesamte Dateisystem wieder her, und zwar aus noch vorhandenen und gelöschten Dateien. Das ist besonders praktisch, wenn man versehentlich das Wurzelverzeichnis oder ein Verzeichnis auf oberster Ebene gelöscht hat.

Findet ext4magic kaum wiederherstellbare Dateien, könnte das an einem zuvor versehentlich gelöschten Journal liegen. Da Sie vor dem Herunterfahren des Rechners eine Kopie gespeichert haben, können Sie es damit versuchen. Dazu rufen Sie `ext4magic` mit dem Parameter `-j` gefolgt vom Dateinamen der Journal-Kopie auf:

```
sudo ext4magic -m \
-j /mnt/ext4.journal -d /mnt \
/dev/mapper/vgubuntu-root
```

Die wiederhergestellten Daten speichert ext4magic im Unterverzeichnis `RECOVERDIR`, und zwar so weit feststellbar mit dem Original-Dateipfad. Für Dateien oder Verzeichnisse, deren Name oder Pfad ext4magic nicht ermitteln kann, verwendet das Programm drei Sonderverzeichnisse: In `MAGIC-1` sind Dateien und Verzeichnisse mit der Inode-Nummer benannt und in den Verzeichnissen `MAGIC-2` und `MAGIC-3` sind die Dateien anhand des erkannten Dateityps sortiert.

Die Typenerkennung ist allerdings ziemlich unzuverlässig. Erinnern Sie sich noch an einen Teil der vermissten Datei, etwa an eine bestimmte Textzeile in einem Dokument oder an einen Funktionsnamen in einer Quellcode-Datei, dann haben Sie gute Chancen, die Datei mittels `find` in den magischen Verzeichnissen aufzuspüren:

```
find /mnt/RECOVERDIR -type f -exec \
grep -l 'def getVisualization' {} \;
```

Der Befehl sucht nach einer Python-Datei, in der die Funktion `getVisualization` definiert ist, und listet deren Dateipfad auf. Entscheidend ist, dass Sie das Semikolon am Ende der Zeile mit einem Backslash schützen, denn nur so interpretiert `find` es als Ende des auszuführenden Befehls.

Fazit

Mithilfe des Journals zaubert ext4magic Dateien wieder hervor, die man eigentlich schon verloren geglaubt hatte. Die Voraussetzung ist aber, dass Sie im Fall der Fälle einen klaren Kopf behalten und die To-do-Liste für gelöschte Dateien gewissenhaft Punkt für Punkt abarbeiten. Da ext4magic den Löschzeitpunkt als Suchmerkmal einbeziehen kann, erreichen Sie damit oft schneller bessere Ergebnisse als mit forensischen Programmen wie PhotoRec, TestDisk oder foremost, die sich auf der gesamten Festplatte auf stoische Mustersuche begeben. So rettet Ihnen ext4magic im Zweifel nicht nur Ihren Job, sondern sogar Ihren wohlverdienten Feierabend. (mid) c't

Vorschau: c't Sicher einkaufen

Digital bezahlen, richtig reklamieren, Betrug erkennen

Ab 22. August im Handel und auf ct.de

Einkaufen und das so sicher wie möglich: Insbesondere im Internet lauern beim Shopping einige Fußangeln, von Cyberkriminalität ganz abgesehen. Gut informiert können Verbraucher vielen davon jedoch aus dem Weg gehen.

Den Anfang in diesem c't-Sonderheft macht die Auswahl des Shops: Worauf sollten Onlineshopper achten, wenn sie Preisvergleiche nutzen und nach Schnäppchen suchen, damit sich der Händler nicht als Fakeshop entpuppt? Und wie können sie ihre Kundenkarten effizient digitalisieren?

Im zweiten Schritt stellen wir Bezahlverfahren und ihre Vor- und Nachteile vor. Wir erklären, was es mit dem Trend zu Debitkarten von Visa und Mastercard auf sich hat und worin die Unterschiede zur deutschen Girocard bestehen – und was Smartphone-Wallets besser können als Plastikkarten.

Da die meisten Probleme nach dem Kauf auftreten, geben wir auch Tipps zu Reklamationen und Rückabwicklungen sowie zu Ratenkäufen und Schufa. Last, but not least erklären wir gängige Betrugsmaschen im Internet, von Fallen auf Kleinanzeigen.de bis zum Onlinebanking-Betrug.

Bild: iStock - Blue Planet Studio

Weitere Infos: ct.de/wxhu

Themenschwerpunkte

Online einkaufen
- Checklisten: Preisvergleicher, Schnäppchen-Portale, Shops
- digitale Kundenkarten

Digital bezahlen
- Checkliste: Bezahlverfahren im Vergleich
- Debitkarte und Girocard
- Wallets für Smartphone und Smartwatch
- Giropay und PayPal
- Bezahlen im Ausland

Kaufprobleme lösen
- Vorsicht-Kunde-Klassiker
- Reklamationen
- Rückabwicklungen
- Chargebacks bei Kreditkarten
- Rechnungs- und Ratenkauf
- Schufa-Basics

Betrug verhindern
- Anti-Fakeshop-Tools
- Betrug auf Kleinanzeigenportalen
- Fußangeln beim PayPal-Käuferschutz
- Telefonbetrug im Onlinebanking

Container orchestrieren in der Praxis

Heft + PDF mit 28 % Rabatt

Mit Kubernetes haben Sie Zugriff auf ein mächtiges Werkzeug zur Containerorchestrierung inklusive riesigem Open-Source-Ökosystem.
Dieses c't-Sonderheft richtet sich an alle, die schon mit Containern arbeiten, Admins wie Entwickler gleichermaßen. Wir reichen Ihnen das komplette Handwerkszeug, um Ihren ersten Kubernetes-Cluster einzurichten und zeigen erprobte Strategien aus der Praxis für Storage und vieles mehr:

- Der Lernpfad zum Kubernetes-Kenner
- Docker und Podman im DevOps-Alltag
- GitOps: Automatische Clusterverwaltung mit Helm und Argo CD
- Kubernetes-Praxis für Container-Profis
- Schlanke Cluster On-Premises und in der Cloud
- Auch als Paket-Angebot Heft + digitale Ausgabe + Fachbuch "Kubernetes" vom dpunkt-Verlag

Heft für 22,50 € • PDF für 19,90 € • Bundle Heft + PDF 30,50 €

shop.heise.de/ct-kubernetes

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 € (innerhalb Deutschlands). Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

heise Shop

B1 Consulting Managed Service & Support

individuell – umfassend – kundenorientiert

Neue oder bestehende Systemlandschaften stellen hohe Anforderungen an Ihr IT-Personal. Mit einem individuellen Support- und Betriebsvertrag von B1 Systems ergänzen Sie Ihr Team um die Erfahrung und das Wissen unserer über 150 festangestellten Linux- und Open-Source-Experten.

Unsere Kernthemen:

Linux Server & Desktop · Private Cloud (OpenStack & Ceph) · Public Cloud (AWS, Azure, OTC & GCP) · Container (Docker, Kubernetes, Red Hat OpenShift & Rancher) · Monitoring (Icinga, Nagios & ELK) · Patch Management · Automatisierung (Ansible, Salt, Puppet & Chef) · Videokonferenzen

Unser in Deutschland ansässiges Support- und Betriebsteam ist immer für Sie da – mit qualifizierten Reaktionszeiten ab 10 Minuten und Supportzeiten von 8x5 bis 24x7!

B1 SYSTEMS

B1 Systems GmbH - Ihr Linux-Partner

Linux/Open Source Consulting, Training, Managed Service & Support

ROCKOLDING · KÖLN · BERLIN · DRESDEN · JENA

www.b1-systems.de · info@b1-systems.de