

Untermieter verkabeln

Das Netzwerk virtueller Maschinen unter Linux individuell anpassen

Unter Linux richten Gnome Boxes oder Virt-Manager schnell und komfortabel virtuelle Maschinen (VMs) ein. Die Netzwerkkonfiguration erfordert aber etwas Tüftelei. Dieser Artikel liefert das nötige Rüstzeug, um Ihre Untermieter passend zu verbinden.

Von Keywan Tonekaboni

Dank QEMU und KVM in heutigen Distributionen sind virtuelle Maschinen (VMs) mit Linux in Nullkommanichts am Start. Dabei helfen entweder Gnome Boxes oder Virt-Manager als Oberfläche auf dem Wirt beim Konfigurieren und Bedienen; das haben wir bereits in [1] erklärt. Beide bringen eine Minimalausstattung für die „Vernetzung“ der VMs mit. Die genügt zumindest, um das virtuelle Betriebssystem mit dem Internet zu verbinden, wenn denn der Wirt selbst angeschlossen ist.

Sie bedienen sich dazu eines einfachen Tricks: Der Wirt dient quasi als Router. Er gibt den Netzwerkverkehr der VMs als seinen eigenen aus und verteilt eingehende Antworten wieder an die VMs – man spricht dann auch von Network Address Translation (NAT). Aus Sicht des Netzwerks verstecken sich die VMs hinter dem Wirt; sie nutzen IP-Adressen aus einem anderen Bereich als der Wirt. Dadurch sind solche VMs für das übrige Netzwerk auch nicht erreichbar. Die Art der Konfiguration eignet sich also nicht, um Dienste aus einer VM heraus im lokalen Netzwerk anzubieten, etwa Nextcloud dort laufen zu lassen.

Alternativ kann ein Wirt auch die Netzwerkschnittstelle einer VM zusätzlich zu seiner eigenen in das lokale Netz verlegen. Die VM sieht aus Sicht des Netzwerks dann aus wie ein weiteres System, das eben neben dem Wirt dort angeschlossen ist. Der technische Begriff dafür ist Bridge – der Wirt

bildet mit seiner Netzwerkschnittstelle eine Brücke, über die die VM ihren Netzwerkverkehr leiten kann. Solche VMs sind für das übrige Netzwerk erreichbar, ein in der VM laufender Dienst wie Nextcloud wäre für andere nutzbar. Die VM erhält IP-Adressen aus dem gleichen Bereich wie der Wirt. Die VMs stecken quasi im gleichen Netz.

Virtuelle Netze

Ein Blick auf die Technik dahinter: Etwas verwirrend ist, dass Virtualisierungssoftware unter Linux für die Implementierung dieser Funktionen auf eine Kernel-Komponente namens Bridge zurückgreifen kann. Sie implementiert einen virtuellen Switch, mit dem man physische und logische Netzwerkkomponenten verbinden kann: Wie in einem realen Switch steckt man per Software die Geräte physischer Netzwerkkarten dort hinein und ebenso logische Geräte, die mit der Netzwerkkarte in einer VM verbunden sind. So entstehen virtuelle Netze, in der alle Beteiligten wie in einem realen Netz verschaltet sind.

Gnome Boxes verwendet die Linux-Bridge nicht. Virt-Manager und die als Rückgrat der Netzwerkkonfiguration verwendete Infrastruktur der Libvirt verwenden sie in spezieller Weise: Sie errichten

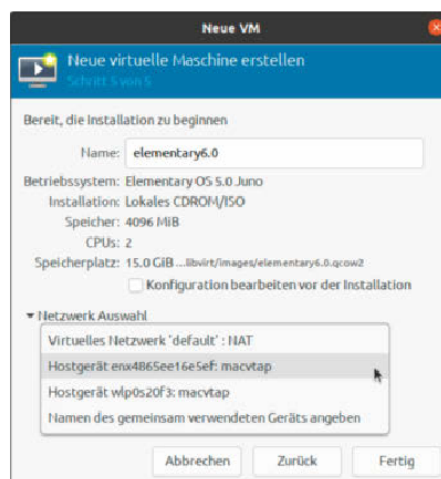
damit virtuelle Netzwerke, die private IP-Adressen verwenden und vom Wirt per NAT mit der Welt verbunden werden. Ob der Host Teil des virtuellen Netzes ist, entscheidet, ob er mit den VMs via Netzwerk Kontakt aufnehmen kann oder nicht. Aus Sicht des Netzes vor dem Host sind die VMs nicht erreichbar.

Alternativ kann eine Linux-Bridge auch die (physische) Netzwerkkarte des Wirts aufnehmen. Dann wären alle dort „eingesteckten“ Geräte, also VMs und Host nebeneinander im Netz. Alle wären von außen erreichbar. Allerdings bietet Libvirt und somit weder Gnome Boxes noch Virt-Manager das Einrichten einer derart konfigurierten Linux-Bridge an. Wer eine solche Konfiguration einrichten will, muss deshalb die Netzwerkkonfiguration seiner Linux-Distribution so anpassen, dass diese beim Systemstart eine geeignete Linux-Bridge hochfährt.

Virt-Manager verwendet eine andere Technik, um die Netzwerkschnittstelle einer VM mit der Netzwerkkarte des Hosts kurz-zuschließen: Macvtap. Die Netzwerkkarte des Wirts erhält eine zweite MAC-Adresse, sodass sie sich aus Sicht des Netzwerkes wie eine zweite Netzwerkkarte verhält. Die dort landenden Pakete werden dann in die VM hineingereicht. Wie hinter einer Linux-Bridge können auf diese Weise „vernetzte“ VMs beliebig miteinander kommunizieren. Allerdings sind Wirt und VMs mit Macvtap untereinander nicht erreichbar.

Einfache Vernetzung

Die einfachste Möglichkeit, eine VM das Netzwerk des Wirts nutzen zu lassen, wählt Gnome Boxes. Ohne dass der Nutzer spezielle Rechte braucht, verpasst es der Netzwerkkarte jeder VM eine private IP-Adresse und sorgt per NAT dafür, dass Anwendungen in der VM von der Anbindung des Wirts profitieren. Der VM stehen damit alle Netzwerkverbindungen des Wirts offen – einschließlich etwaiger VPN-Verbindungen. Laufen mehrere VMs, können die einander nicht erreichen. Der Host ist aber für alle VMs ansprechbar.



Die Auswahl des Netzwerkes im Virt-Manager entscheidet, ob und wie VMs, Wirt und Außenwelt erreichbar sind.

Hinter den Kulissen bemüht Gnome Boxes dazu Libvirt-Funktionen in einem speziellen Kontext namens „qemu:///session“. Sie stellen für jeden Benutzer eines Systems eine separate Umgebung zum Ausführen von VMs bereit. Der Nutzer benötigt keine erweiterten Rechte und sieht nur seine eigenen VMs. Entsprechend laufen die VMs auch nur, wenn der Nutzer angemeldet und Gnome Boxes gestartet ist.

Standardmäßig kommen VMs dann per „User Networking“ ins Netz. Die Technik gilt als lahm und erlaubt nur mit Tricks Anwendungen wie Ping – die Distributionen sind in der Regel passend voreingestellt, sodass man als Nutzer nicht aktiv werden muss. Kurzum: Gerade für Netzwerkdienste, die man dem Netz bereitstellen will, ist Gnome Boxes ungeeignet. Auch reparieren kann man da wenig, da die Netzwerkanbindung an allen regulären Techniken eines Linux-Systems vorbeiläuft, etwa der Firewall des Wirtes mit Funktionen für NAT und mehr.

Theoretisch erlaubt das im Hintergrund arbeitende Libvirt auch, im Kontext von „qemu:///session“ ausgeführte VMs mit einer Linux-Bridge zu verbinden. Dazu muss man QEMU erlauben, Geräte in eine solche Bridge zu stecken, und ein Helferskript so konfigurieren, dass es mit Root-Rechten ausgeführt wird. Unterm Strich ist das aber viel Aufwand, den Gnome Boxes nicht würdigt – lediglich aktuelle Versionen erlauben via integriertem XML-Editor die Konfiguration entsprechend zu modifizieren; mit der grafischen Oberfläche geht das nicht.

Anspruchsvollere Netze

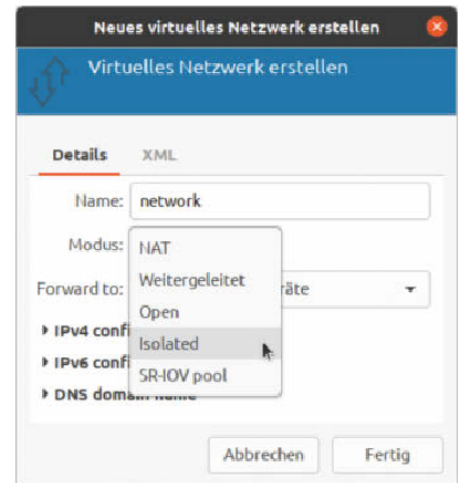
Der Virt-Manager wählt von sich aus einen anderen Libvirt-Kontext namens „qemu:///system“. Hierfür würde ein regulärer Nutzer Root-Rechte benötigen. Eine trickreiche Konfiguration über das

PolicyKit reduziert die Anforderung darauf, dass der Nutzer Mitglied in der Gruppe libvirt sein muss, und erspart so die Passwordeingabe beim Start des Virt-Managers und beim Ändern der Netzwerkkonfiguration. Ja: Mit Virt-Manager können Sie beliebig viele virtuelle Netzwerke einrichten und die VMs mit ihnen verbinden – ein weiterer Vorteil gegenüber Gnome Boxes bei der Vernetzung von VMs.

Die grafische Oberfläche des Virt-Managers richtet Linux-Bridges stets so ein, dass sich die VMs per NAT hinter dem Wirt verstecken. Sollen die VMs parallel zum Wirt im Netz erscheinen, bietet Virt-Manager in der Detailkonfiguration virtueller Netzwerkkarten für die VM die physischen Karten des Wirts als „Hostgerät <xyz> macvtap“ an. So gelangen die VMs neben dem Wirt ins lokale Netz.

Diese Brückenbildung via Macvtap hat mehrere Nachteile: Sie gelingt bei den allermeisten WLAN-Adaptoren nicht. Virt-Manager bietet die Karten zwar an, aber die VM erhält dann keine Adressen. In solchen Fällen bleibt nur die Verbindung der VM-Netzwerkkarte mit einem virtuellen NAT-Netzwerk. Wie eingangs schon erwähnt und vom Virt-Manager auch bei der Auswahl eines Macvtap-Geräts angezeigt, können Wirt und VM darüber nicht kommunizieren. Hier kann man sich mit einer zweiten Netzwerkkarte helfen, die den NAT-Modus verwendet.

Zum Anlegen weiterer Netzwerke gelangen Sie aus dem Hauptfenster des Virt-Managers unter „Bearbeiten“ der „Verbindungsdetails“. Alle dort im Reiter „Virtuelles Netzwerk“ angelegten Netzwerke erzeugen eine Linux-Bridge, also letztlich einen virtuellen Switch. Diese Linux-Bridges richtet Libvirt beim Systemstart unabhängig von Benutzeranmeldungen ein. Jedem dieser virtuellen Netzwerke weist Virt-Manager ein eigenes IPv4-



Virt-Manager hilft dabei, eine einfache Netzwerkbrücke anzulegen. Der Modus legt fest, welche Regeln Libvirt in der Firewall anlegt.

Netz zu; IPv6-Netze muss man von Hand aktivieren.

Sollen nur Wirt und VMs miteinander kommunizieren, kann man die NAT-Konfiguration auch auf das Loopback-Interface (lo) begrenzen. Neben der standardmäßig vorgegebenen NAT-Konfiguration kann man auch Netze einrichten, in denen der Wirt nicht mitspielen darf (Isolated). Bei den Spielarten „Open“ und „Weitergeleitet“ muss man selbst die Firewall und das Netzwerk außerhalb des Wirts nach eigenen Wünschen konfigurieren. Das ist tendenziell etwas für Netzwerkprofis. Das gilt auch für die letzte Option „SR-IOV-Pool“. Die setzt besondere Hardware voraus.

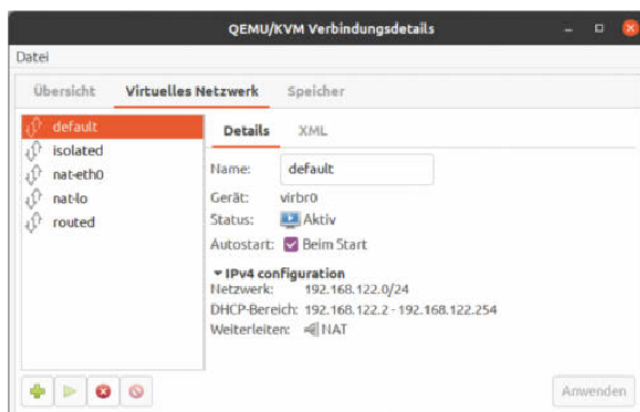
Netze für Experten

Wenn Sie unbedingt eine gleichberechtigte Kommunikation zwischen Wirt und VMs erreichen wollen, kommen Sie einfacher mit einer auf Ihrer Distribution passend eingerichteten Linux-Bridge zum Ziel. Die Dokumentation weist meist einen Weg. Anstatt die IP-Adresse auf dem physischen Netzwerkgerät, etwa eth0, zu beziehen, setzt man diese auf der Bridge. Der Virt-Manager findet solche von Hand an Libvirt vorbei konfigurierten Bridges und bietet sie in der VM-Konfiguration zur Auswahl an. (ktn@ct.de) **ct**

Literatur

- [1] Keywan Tonekaboni, Untermieter, Desktop-Virtualisierung unter Linux einfach und zuverlässig nutzen, c't 2/2021, S. 154

Weitere Infos: ct.de/y2fu



Die in den Verbindungsdetails von Virt-Manager eingerichteten virtuellen Netzwerke weist man den VMs zu.