Rootless QEMU

Thomas Rahimi

Inhalt

Motivation

Hintergrund

- Virtualisierung? Es gibt doch Docker/podman,…?
- Aber …Entwicklungsumgebungen, Sicherheitsanalysen, etc.?
- Tatsächlich, virtuelle Maschinen als Teil vieler Workflows, z. B.
  - Sicherheitsanalysen von Netzwerken mit Kali in einer VM
  - Entwicklungsumgebungen, um das Gastsystem aufgeräumt zu halten

Rootless QEMU

- Nutzer müssen nicht Mitglieder in bestimmten Gruppen sein
- keine Anpassung der Dateiberechtigungen für VMs nötig
- Nutzung auch dann möglich, wenn Nutzer keine Root-Rechte auf Host-System haben sollen oder dürfen

Annahmen

Betriebssystem

- getestet unter OpenSUSE Tumbleweed
- lauffähig wenn Programme in folgenden Versionen vorliegen

Notwendige Programme

Name	Version
QEMU	9.2.2
libvirt-daemon	11.0.0
(passt)	20250217

virt-manager

- Im Folgenden Nutzung der GUI
- aber auch ohne GUI nutzbar

QEMU und libvirt

QEMU

- Userspace für Emulation und Virtualisierung [1]
- Dient als Frontend für verschiedene Virtualisierungsmodule [1], z. B.:
  - KVM
  - Xen

libvirt

- Bereitstellung von:
  - Speicher
  - Netzwerk
  - Verwaltung von kryptographischem Material
  - etc.
- für virtuelle Maschinen

Einrichtung

Verbindung einrichten

1. virt-manager starten
2. neue Verbindung einrichten
3. als Typ: `QEMU/KVM Benutzer-Session` wählen
   - Damit Nutzung von `qemu:///session` [4]
   - Standard: `qemu:///system` braucht Privilegien für ausführende Nutzer [4]
4. Haken für automatisches Verbinden setzen

Und jetzt im Video

Einstellungen

- `XML-Bearbeitung` in den Einstellungen von virt-manager aktivieren
- Wichtig für die Vernetzung der VMs

Netzwerk - Slirp4netns

Erläuterung

- von libvirt nativ bereitgestellt [2]
- keine Konfiguration eines Backends notwendig
- Nicht vorhanden:
  - grafische Nutzeroberfläche in virt-manager
  - Portfreigaben

Beispiel

```
1 <interface type="user">
2 <mac address="52:54:00:3c:bd:a6"/>
3 <ip address="192.168.100.222" family
    ="ipv4"/>
4 <ip address="fc::/10" family="ipv6"
    prefix="64"/>
5  <model type="virtio"/>
6 <address type="pci" domain="0x0000"
    bus="0x01" slot="0x00" function="
    0x0"/>
7 </interface>
```


Netzwerk - passt

Erläuterung

- separates Programm notwendig [3]
- Weiterentwicklung von `pasta` → Userspace-Networking in podman
- Backend muss konfiguriert werden
- Ermöglicht Port-Freigaben
- Kommunikation über socket-Dateien

Anpassungen

- socket-Dateien per Default unter `/run/user/*/libvirt/`
- evtl. Anpassung von `apparmor`-Profil nötig, um Log-Dateien und Sockets zu schreiben
- Diagnose:
  - Start von virtuellen Maschinen scheitert mit „kryptischem“ Fehler von passt

Beispiel

```
<interface type="user">
<mac address="52:54:00:59:d3:1d"/>
<source dev="enp2s0"/>
<ip address="192.168.100.192" family="ipv4"/>
<ip address="fc::/10" family="ipv6" prefix="64"/>
<portForward proto="tcp">
<range start="8123" end="8125"/>
</portForward>
<model type="virtio"/>
<backend type="passt" logFile="/run/user/1000/passt.log"/>
<address type="pci" domain="0x0000" bus="0x01" slot="0x00"
   function="0x0"/>
</interface>
```


Das war's

Vielen Dank für eure Aufmerksamkeit

Viel Erfolg beim Experimentieren mit virtuellen Maschinen

Literatur I

[1] *Introduction — QEMU documentation*. URL: https://www.qemu.org/docs/master/system/introduction.html (besucht am 07. 03. 2025).

[2] *libvirt: Domain XML format*. URL: https://libvirt.org/formatdomain.html#userspace-connection-using-slirp (besucht am 11. 03. 2025).

[3] *libvirt: Domain XML format*. URL: https://libvirt.org/formatdomain.html#userspace-connection-using-passt (besucht am 11. 03. 2025).

Literatur II

[4] Fernando Lozano. *Rootless virtual machines with KVM and QEMU*. Red Hat Developer. Section: Security. 18. Dez. 2024. URL: https://developers.redhat.com/articles/2024/12/18/rootless-virtual-machines-kvm-and-qemu (besucht am 07. 03. 2025).