Engineer Platform

Ran containers on Podman and Quadlet

Deployed a container plane on Podman and Quadlet under systemd rather than Docker, because Docker's default bridge-port publishing can bypass UFW rules — and gave deploys an unprivileged user with one fixed command instead of root.

September 2026

containers under systemd, not above the firewall

Situation. The platform needed somewhere to run application containers. The obvious choice was the industry default, and the obvious choice was wrong for this host in a specific way: it rewrites the kernel's packet-filter rules and publishes container ports above the firewall rules the hardening role installs, so a container quietly becomes reachable from the internet regardless of what the firewall was told.

Task. A container plane had to be chosen that does not bypass the firewall, does not add a second supervisor beside the one already trusted, and does not require a person to be root to ship a release.

Action. The plane is a daemonless container engine driving units generated by the operating system's own supervisor. There is no second process manager: containers are services, they start the way services start, and they are described in the same declarative form as everything else. The containers use host networking with no published ports at all, which removes the firewall-bypass question rather than mitigating it. Units run at the system level rather than rootless, and that is recorded as a trade — it keeps the automation simple and normal, at the cost of the stricter isolation rootless would give, and the note says which way to move if container escape ever matters more than automation simplicity. Deployment was separated from provisioning: root sets up the deployment path once, and thereafter an unprivileged user redeploys by running one fixed script through a scoped rule that permits that command and no arguments. Build the image, restart the service. No root shell, no arbitrary commands.

Result. Containers run under the supervisor that was already trusted, behind the firewall that was already declared, and a routine release uses one scoped command without a root shell. The choice against the default is written down with its reason, which matters more than the choice — the next person will be told to use the default by every article they read.

Bring this experience to your project

Use “Ran containers on Podman and Quadlet” as a starting point for a similar challenge in your organisation. The services behind this work are available for your project. Servers sized for what you actually use, moved into the cloud or back out of it, with the monthly bill worked out first.

Explore our services Get in touch →

Look behind the result

Read the situation, decisions and result in this example. We can discuss which parts transfer to your constraints and which need another approach. Ran containers on Podman and Quadlet — containers under systemd, not above the firewall

Explore our services Get in touch →

Running containers without opening holes in your firewall?

Talk through your project with the engineer responsible for delivery. We agree the scope, price basis and handover in writing before work begins.

Role context: Infrastructure Automation Engineer. It draws on DevOps, Infrastructure, Containers (Docker/Kubernetes), Automation & CI/CD, Linux & Servers and Security. And while you are here, we are rather good at Cloud Infrastructure & Migration, DevOps & CI/CD Automation, Containerization & Orchestration and Security & Access Management.

Get in touch Explore our services

One piece of **a longer record** — and it is all on this site.

Every entry is written the same way: the situation, the task, what we did and what changed.

See the whole record

Define the improvement you need

Bring the deployment path, the operational risks and the people on call. We can scope a change with checks, a recovery route and clear ownership.

See what it costs Get in touch →

Running containers without opening holes in your firewall?

Ask about the decisions behind “Ran containers on Podman and Quadlet”. You will speak with the people who can explain the work and assess your own project.

Explore our services

welcome@engineer.company +45 50 10 61 84 Copenhagen, Denmark

Take this page with you

Contact card

Carefully Crafted With Love by D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Copyright © 2025 – present · Engineer ApS · All rights reserved.

Printed from https://platform.engineer.company/portfolio/ran-containers-on-podman-and-quadlet/