Engineer Plattform

Kjørte containere på Podman og Quadlet

Satte et containerlag på Podman og Quadlet under systemd i produksjon i stedet for Docker, fordi Dockers standardpublisering av porter på bridge-nettverk kan omgå UFW-regler — og ga produksjonssettinger en uprivilegert bruker med én fast kommando i stedet for root.

september 2026

containere under systemd, ikke over brannmuren

Situasjon. Plattformen trengte et sted å kjøre applikasjonscontainere. Det åpenbare valget var bransjestandarden, og det åpenbare valget var feil for denne verten på en helt bestemt måte: den skriver om kjernens regler i pakkefilteret og publiserer containerporter over brannmurreglene som herdingsrollen installerer, slik at en container i det stille blir tilgjengelig fra internett uansett hva brannmuren har fått beskjed om.

Oppgave. Det måtte velges et containerlag som ikke går utenom brannmuren, ikke legger til en ekstra tjenestestyrer ved siden av den som allerede er betrodd, og ikke krever at en person er root for å levere en utgivelse.

Handling. Laget er en daemonløs containermotor som driver enheter generert av operativsystemets egen tjenestestyrer. Det finnes ingen ekstra prosessbehandler: containere er tjenester, de starter slik tjenester starter, og de beskrives i den samme deklarative formen som alt annet. Containerne bruker vertens nettverk uten noen publiserte porter i det hele tatt, og det fjerner spørsmålet om å gå utenom brannmuren i stedet for å avbøte det. Enhetene kjører på systemnivå og ikke rootless, og det er dokumentert som en avveining — det holder automatiseringen enkel og normal, på bekostning av den strengere isoleringen rootless ville gitt, og notatet sier hvilken vei man skal gå hvis utbrudd fra containeren noen gang blir viktigere enn enkel automatisering. Produksjonssetting ble skilt fra provisjonering: root setter opp stien for produksjonssetting én gang, og deretter setter en uprivilegert bruker i produksjon på nytt ved å kjøre ett fast skript gjennom en avgrenset regel som tillater den kommandoen og ingen argumenter. Bygg imaget, start tjenesten på nytt. Ingen root-shell, ingen vilkårlige kommandoer.

Resultat. Containerne kjører under tjenestestyreren som allerede var betrodd, bak brannmuren som allerede var deklarert, og en rutinemessig utgivelse bruker én avgrenset kommando uten et root-skall. Valget mot standarden er skrevet ned med begrunnelse, og det betyr mer enn selve valget — den neste som kommer, vil få beskjed om å bruke standarden av hver eneste artikkel vedkommende leser.

Bruk erfaringen i prosjektet deres

Bruk «Kjørte containere på Podman og Quadlet» som utgangspunkt for en lignende utfordring i organisasjonen deres. Tjenestene bak arbeidet er tilgjengelige for prosjektet deres. Servere dimensjonert etter det du faktisk bruker, flyttet inn i skyen eller ut av den igjen, med månedsregningen regnet ut på forhånd.

Se tjenestene våre Ta kontakt →

Se bak resultatet

Les om situasjonen, beslutningene og resultatet i eksemplet. Vi kan drøfte hva som passer deres rammer, og hva som krever en annen tilnærming. Kjørte containere på Podman og Quadlet — containere under systemd, ikke over brannmuren

Se tjenestene våre Ta kontakt →

Kjører du containere uten å lage hull i brannmuren?

Snakk om prosjektet med ingeniøren som har ansvaret for leveransen. Vi avtaler omfang, prisgrunnlag og overlevering skriftlig før arbeidet begynner.

Rolle i oppdraget: Ingeniør for infrastrukturautomatisering. Det bygger på DevOps, Infrastruktur, Containere (Docker/Kubernetes), Automatisering og CI/CD, Linux og servere og Sikkerhet. Og nå som dere er her: vi er ganske gode på Skyinfrastruktur og migrering, DevOps og CI/CD-automatisering, Containerisering og orkestrering og Sikkerhet og tilgangsstyring.

Ta kontakt Se tjenestene våre

Ett stykke av **en lengre oversikt** — og den ligger i sin helhet her.

Hver oppføring er skrevet på samme måte: situasjonen, oppgaven, hva vi gjorde, og hva som endret seg.

Se hele oversikten

Definer forbedringen dere trenger

Ta med utrullingsløpet, driftsrisikoene og dem som har vakt. Vi kan avgrense en endring med kontroller, en vei tilbake og tydelig ansvar.

Se hva det koster Ta kontakt →

Kjører du containere uten å lage hull i brannmuren?

Spør om beslutningene bak «Kjørte containere på Podman og Quadlet». Dere snakker med folk som kan forklare arbeidet og vurdere deres eget prosjekt.

Se tjenestene våre

welcome@engineer.company +45 50 10 61 84 København, Danmark

Ta med deg denne siden

Visittkort

Laget med kjærlighet av D.

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

Opphavsrett © 2025 – nå · Engineer ApS · Alle rettigheter forbeholdt.

Skrevet ut fra https://platform.engineer.company/nb/portfolio/ran-containers-on-podman-and-quadlet/