Engineer Platform

Har kørt containere på Podman og Quadlet

Har udrullet et containerlag på Podman og Quadlet under systemd i stedet for Docker, fordi Dockers standardpublicering af porte på bridge-netværk kan omgå UFW-regler — og givet udrulninger en uprivilegeret bruger med én fast kommando i stedet for root.

september 2026

containere under systemd, ikke over firewallen

Situation. Platformen havde brug for et sted at køre applikationscontainere. Det oplagte valg var branchestandarden, og det oplagte valg var forkert for denne vært på en helt bestemt måde: den omskriver kernens pakkefilterregler og placerer containerporte over de firewallregler, hærdningsrollen installerer, så en container i al stilhed bliver tilgængelig fra internettet, uanset hvad firewallen har fået at vide.

Opgave. Der skulle vælges et containerlag, som ikke går uden om firewallen, ikke tilføjer endnu en supervisor ved siden af den, der allerede var betroet, og ikke kræver, at en person er root for at sende en release ud.

Handling. Laget er en dæmonløs containermotor, der kører enheder, som genereres af styresystemets egen supervisor. Der er ingen ekstra proceshåndtering: containere er tjenester, de starter, som tjenester starter, og de beskrives i den samme deklarative form som alt andet. Containerne bruger værtens netværk uden nogen publicerede porte overhovedet, og det fjerner spørgsmålet om at omgå firewallen i stedet for blot at afbøde det. Enhederne kører på systemniveau og ikke rootless, og det er noteret som en afvejning — det holder automatiseringen enkel og normal, på bekostning af den strengere isolation, rootless ville give, og noten siger, hvilken vej man skal gå, hvis udbrud fra containere nogensinde kommer til at betyde mere end enkel automatisering. Udrulning blev adskilt fra provisionering: root sætter udrulningsstien op én gang, og derefter udruller en bruger uden privilegier igen ved at køre ét fast script

gennem en afgrænset regel, der tillader netop den kommando og ingen argumenter. Byg imaget, genstart tjenesten. Ingen root-shell, ingen vilkårlige kommandoer.

Resultat. Containere kører under den supervisor, der allerede var betroet, bag den firewall, der allerede var erklæret, og en rutinemæssig release bruger én afgrænset kommando uden en root-shell. Valget imod standarden er skrevet ned med sin begrundelse, og det betyder mere end selve valget — den næste person vil få at vide, at man skal bruge standarden, af hver eneste artikel, vedkommende læser.

Brug erfaringen i jeres projekt

Brug »Har kørt containere på Podman og Quadlet« som udgangspunkt for en lignende udfordring i jeres organisation. Ydelserne bag arbejdet kan også bruges i jeres projekt. Servere dimensioneret efter det, I rent faktisk bruger, flyttet op i skyen eller hjem igen, med den månedlige regning regnet ud først.

Se vores ydelser Kontakt os →

Se bag resultatet

Læs om situationen, beslutningerne og resultatet i eksemplet. Vi kan drøfte, hvad der passer til jeres vilkår, og hvad der kræver en anden tilgang. Har kørt containere på Podman og Quadlet — containere under systemd, ikke over firewallen

Se vores ydelser Kontakt os →

Kører du containere uden at åbne huller i din firewall?

Tal om jeres projekt med den ingeniør, der har ansvaret for leverancen. Vi aftaler omfang, prisgrundlag og overdragelse skriftligt, før arbejdet begynder.

Rolle i opgaven: Infrastrukturautomatiseringsingeniør. Det trækker på DevOps, Infrastruktur, Containere (Docker/Kubernetes), Automatisering & CI/CD, Linux & servere og Sikkerhed. Og når I alligevel er her, er vi ret dygtige til Cloud-infrastruktur & migrering, DevOps & CI/CD-automatisering, Containerisering & orkestrering og Sikkerhed & adgangsstyring.

Kontakt os Se vores ydelser

Ét stykke af **en længere fortegnelse** — og det hele ligger her på sitet.

Hver post er skrevet på samme måde: situationen, opgaven, hvad vi gjorde, og hvad der ændrede sig.

Se hele fortegnelsen

Definér den ønskede forbedring

Medbring udrulningsforløbet, driftsrisiciene og dem, der har vagten. Vi kan afgrænse en ændring med kontroller, en vej tilbage og tydeligt ansvar.

Se, hvad det koster Kontakt os →

Kører du containere uden at åbne huller i din firewall?

Spørg til beslutningerne bag »Har kørt containere på Podman og Quadlet«. I taler med mennesker, der kan forklare arbejdet og vurdere jeres eget projekt.

Se vores ydelser

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

Tag denne side med dig

Visitkort

Lavet med kærlighed af D.

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

Copyright © 2025 – nu · Engineer ApS · Alle rettigheder forbeholdes.

Udskrevet fra https://platform.engineer.company/da/portfolio/ran-containers-on-podman-and-quadlet/