Engineer

Körde containrar på Podman och Quadlet

Driftsatte en containermiljö på Podman och Quadlet under systemd i stället för Docker, eftersom Dockers standardpublicering av portar i bridge-nätverk kan kringgå UFW-regler — och gav driftsättningarna en oprivilegierad användare med ett enda fast kommando i stället för root.

september 2026

containrar under systemd, inte ovanför brandväggen

Situation. Plattformen behövde någonstans att köra applikationscontainrar. Det självklara valet var branschens standard, och det självklara valet var fel för den här värden på ett specifikt sätt: det skriver om reglerna i kärnans paketfilter och publicerar containerportar ovanför de brandväggsregler som härdningsrollen installerar, så att en container i tysthet blir nåbar från internet oavsett vad brandväggen har instruerats att göra.

Uppgift. Ett containerskikt måste väljas som inte kringgår brandväggen, inte lägger till en andra tjänstehanterare bredvid den som redan är betrodd och inte kräver att en person är root för att göra en release.

Handling. Skiktet är en containermotor utan daemon som driver enheter genererade av operativsystemets egen tjänstehanterare. Det finns ingen andra processhanterare: containrar är tjänster, de startar på samma sätt som tjänster startar och de beskrivs i samma deklarativa form som allt annat. Containrarna använder värdnätverk utan några publicerade portar alls, vilket tar bort frågan om att kringgå brandväggen i stället för att mildra den. Enheterna körs på systemnivå snarare än rootless, och det är nedskrivet som en avvägning — det håller automatiseringen enkel och normal, till priset av den striktare isolering som rootless skulle ge, och anteckningen säger åt vilket håll man ska gå om containerutbrytning någon gång blir viktigare än en enkel automatisering. Driftsättning skildes från provisionering: root förbereder driftsättningsvägen en gång, och därefter driftsätter en oprivilegierad användare på nytt genom att köra ett enda fast skript via en avgränsad regel som tillåter just det kommandot och inga argument. Bygg avbildningen, starta om tjänsten. Inget root-skal, inga godtyckliga kommandon.

Resultat. Containrar körs under den tjänstehanterare som redan var betrodd, bakom den brandvägg som redan var deklarerad, och en rutinmässig release använder ett avgränsat kommando utan ett root-skal. Valet mot standarden är nedskrivet med sitt skäl, vilket väger tyngre än själva valet — nästa person kommer att få höra att standarden ska användas i varenda artikel som den personen läser.

Använd erfarenheten i ert projekt

Använd ”Körde containrar på Podman och Quadlet” som utgångspunkt för en liknande utmaning i er organisation. Tjänsterna bakom arbetet finns tillgängliga för ert projekt. Servrar dimensionerade efter vad du faktiskt använder, flyttade till molnet eller tillbaka ut ur det, med månadskostnaden uträknad först.

Se våra tjänster Hör av er →

Se bakom resultatet

Läs om situationen, besluten och resultatet i exemplet. Vi kan diskutera vad som passar era förutsättningar och vad som kräver ett annat angreppssätt. Körde containrar på Podman och Quadlet — containrar under systemd, inte ovanför brandväggen

Se våra tjänster Hör av er →

Kör du containrar utan att öppna hål i brandväggen?

Prata om ert projekt med ingenjören som ansvarar för leveransen. Vi avtalar omfattning, hur priset beräknas och överlämning skriftligt innan arbetet börjar.

Roll i uppdraget: Ingenjör inom infrastrukturautomation. Det bygger på DevOps, Infrastruktur, Containrar (Docker/Kubernetes), Automatisering och CI/CD, Linux och servrar och Säkerhet. Och nu när ni är här: vi är ganska bra på Molninfrastruktur och migrering, DevOps och CI/CD-automatisering, Containerisering och orkestrering och Säkerhet och behörighetshantering.

Hör av er Se våra tjänster

En del av **en längre historik** — och den finns i sin helhet här.

Varje post är skriven på samma sätt: situationen, uppgiften, vad vi gjorde och vad som förändrades.

Se hela historiken

Definiera förbättringen ni behöver

Ta med driftsättningsvägen, driftsriskerna och dem som har jour. Vi kan avgränsa en förändring med kontroller, en väg tillbaka och tydligt ansvar.

Se vad det kostar Hör av er →

Kör du containrar utan att öppna hål i brandväggen?

Fråga om besluten bakom ”Körde containrar på Podman och Quadlet”. Ni talar med personer som kan förklara arbetet och bedöma ert eget projekt.

Se våra tjänster

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

Ta med dig den här sidan

Visitkort

Omsorgsfullt skapad med kärlek av D.

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

Upphovsrätt © 2025 – nu · Engineer ApS · Alla rättigheter förbehållna.

Utskrivet från https://engineer.company/sv/portfolio/ran-containers-on-podman-and-quadlet/